Fraunhofer SIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Universität Regensburg

Universität Bremen

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Der digitale Nachlass

Eine Untersuchung aus rechtlicher und technischer Sicht

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

Bundesanstalt für Landwirtschaft und Ernährung

ptble
Projektträger Bundesanstalt für Landwirtschaft und Ernährung

aufgrund eines Beschlusses des Deutschen Bundestages

Der digitale Nachlass

Impressum

Kontaktadresse
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Hrsg.: Fraunhofer SIT, Universität Bremen/IGMR, Universität Regensburg

Digital Object Identifier (DOI)
10.24406/sit-n-572149 https://doi.org/10.24406/sit-n-572149

Druck und Weiterverarbeitung
Mediendienstleistungen des Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart

Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

Bildnachweis: Titelbild © iStockphoto / freepik

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75, 64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Der digitale Nachlass

Eine Untersuchung aus rechtlicher und technischer Sicht

27. Dezember 2019

Herausgeber:
Fraunhofer-Institut für Sichere Informationstechnologie
Universität Bremen/IGMR
Universität Regensburg

Autoren:
Marcel Kubis, Universität Bremen
Magdalena Naczinsky, Universität Regensburg
Annika Selzer, Fraunhofer SIT
Tim Sperlich, Universität Bremen
Simone Steiner, Fraunhofer SIT
Ulrich Waldmann, Fraunhofer SIT

Christine Lambrecht
Bundesministerin der Justiz
und für Verbraucherschutz

Vorwort zur Studie zum digitalen Nachlass

Die digitale Welt nimmt einen immer größeren Raum in unserem Leben ein. Die Nutzung des Internets ist selbstverständlich geworden, ein Leben ohne soziale Medien und Smartphones ist für viele nicht mehr vorstellbar. Überall in der digitalen Welt hinterlassen Nutzerinnen und Nutzer Spuren. Viele richten ein Facebook-Profil ein, schließen online Verträge ab, nutzen die Möglichkeiten des E-Banking, „kaufen“ E-Books oder laden kostenpflichtig Musiktitel herunter.

Den meisten Menschen fällt es schwer, sich mit der Frage zu befassen, was nach ihrem Tod mit ihrem Nachlass geschehen soll. Noch weniger Menschen machen sich Gedanken darüber, dass zum Vermögen auch der digitale Nachlass gehört. So kommt es, dass häufig hierfür keine Vorsorge getroffen wird.

Der Bundesgerichtshof hat zur Vererblichkeit von Nutzungsverträgen mit sozialen Netzwerken festgestellt, dass das Erbrecht des Bürgerlichen Gesetzbuchs auch für den digitalen Nachlass uneingeschränkt Anwendung findet. Danach rückt der Erbe auch hinsichtlich des digitalen Nachlasses vollständig in die Stellung des Erblassers ein. Auch wenn damit die grundlegenden erbrechtlichen Fragen weitgehend geklärt sind, stellen sich in diesem Zusammenhang für die Verbraucherinnen und Verbraucher eine Reihe weiterer Fragen:

Was gehört überhaupt zum digitalen Nachlass? Was geschieht mit den durch die Nutzung von IT-Systemen entstandenen Daten? Wie kann ich als Erbe bei den Dienstanbietern mein Recht auf Zugang zu den digitalen Inhalten durchsetzen? Wie kann ich Vorsorge treffen, sodass meine Erben unkompliziert an meinen digitalen Nachlass gelangen? Wie kann ich umgekehrt verhindern, dass irgendjemand nach meinem Tode von meinen Daten Kenntnis erlangt?

Für das Bundesministerium der Justiz und für Verbraucherschutz ist die Verbraucheraufklärung ein zentrales Anliegen. Wir wollen den Verbraucherinnen und Verbrauchern auch auf dem Gebiet des digitalen Nachlasses Orientierung und Hilfestellung anbieten. Daher haben wir das Forschungsvorhaben des Fraunhofer-Instituts für Sichere Informationstechnologie und der Universitäten Regensburg und Bremen gerne gefördert.

Die Studie bereitet die im Zusammenhang mit dem digitalen Nachlass stehenden Fragestellungen aus rechtswissenschaftlicher Perspektive auf. Dabei stehen verbraucherrechtliche, datenschutzrechtliche, erbrechtliche und urheberrechtliche Fragestellungen im Vordergrund. Sie befasst sich aber auch mit den technischen Aspekten der Thematik. Untersucht wurde außerdem, ob gesetzgeberischer Handlungsbedarf besteht. Dies wird weitgehend verneint. Stattdessen enthält die Studie eine Reihe von praktischen Hinweisen, wie Nutzer von Online-Diensten nicht nur für den Fall des Todes vorsorgen können, sondern auch für den Fall ihrer rechtlichen Handlungsunfähigkeit, z. B. nach einem schweren Unfall. Eingeschlossen sind konkrete Handlungsempfehlungen für Online-Dienste, Erblasser, Erben, Vorsorgebevollmächtigte, Betreuer, wie auch die Verwaltung. Zudem werden für die Vorsorgevollmacht und Verfügungen von Todes wegen Textvorlagen vorgestellt.

Wir werden die Empfehlungen zur Verbesserung der Verbraucherfreundlichkeit bei der Vererbung digitaler Werte gezielt auswerten und prüfen, inwieweit weitere Maßnahmen zum Schutz der Verbraucherinnen und Verbraucher in diesem Bereich notwendig sind.

Die vorliegende umfassende Studie ist damit ein wichtiger Baustein für eine verbesserte Information im Bereich des digitalen Nachlasses.

Christine Lambrecht

Bundesministerin der Justiz
und für Verbraucherschutz

Vorwort der beteiligten Forschungseinrichtungen

Nur wenige Menschen wissen, dass und wie sie über ihren digitalen Nachlass verfügen können. Obwohl sich jeder zwangsläufig irgendwann in seinem Leben auch mit Nachlassfragen beschäftigen muss bzw. sollte, wissen viele nicht, was ein digitaler Nachlass ist, welche Daten, Vertragsbeziehungen und Nutzungsrechte damit verbunden sind und ob das Thema für sie überhaupt relevant werden könnte. Hinzu kommt, dass viele Verträge über digitale Produkte durch die starke wirtschaftliche Stellung der Anbieter einseitig zu Ungunsten der Verbraucher ausgestaltet sind. Die AGB-Regelungen in diesen Verträgen mögen rechtskonform sein, sind aber dennoch nicht verbraucherfreundlich und sehen meist auch keine Optionen für den digitalen Nachlass vor.

Vor diesem Hintergrund haben die drei Projektpartner Fraunhofer SIT, Uni Bremen und Uni Regensburg von Mai bis Dezember 2019 das Thema des digitalen Nachlasses aus rechtswissenschaftlicher und technischer Sicht aufbereitet. Ziel der Studie ist es unter anderem aufzuzeigen, welche Möglichkeiten zur Vorsorge für den digitalen Nachlass bestehen und welche Benachteiligungen aus Verbrauchersicht beim digitalen Nachlass derzeit zu befürchten sind, sowie Empfehlungen zu geben, wie im Sinne einer Verbraucherfreundlichkeit die Vererbbarkeit digitaler Werte verbessert werden kann. Betrachtet werden diese Fragen sowohl aus Sicht des Erb-, Datenschutz-, Urheber- und Verbraucherschutzrechts als auch aus Sicht der Technik.

In insgesamt neun Kapiteln befasst sich die Studie u. a. mit den Fragen, welche Werte den digitalen Nachlass einer Person bilden, ob und wie digitale Inhalte vererbbar sind, ob ein absolutes Recht an personenbezogenen Daten notwendig ist, inwiefern es derzeit ein „postmortales Datenschutzrecht“ gibt und ob dieses erweitert werden muss, ob Anbieter digitaler Werte Verbraucherinnen und Verbraucher mit ihren Vertragsregelungen zum digitalen Nachlass unangemessen benachteiligen und wie sich die Vorsorge eines digitalen Nachlasses technisch unterstützen lässt.

Die vorliegende Studie wurde durch das Bundesministerium der Justiz und für Verbraucherschutz gefördert, dem wir auf diesem Wege unseren Dank für die Unterstützung der Forschungsarbeiten ausdrücken möchten.

Prof. Dr. Benedikt Buchner	Prof. Dr. Martin Löhnig	Prof. Dr. Michael Waidner
Universität Bremen	Universität Regensburg	Fraunhofer SIT

Inhaltsverzeichnis

Zusammenfassung der Studie

Warum diese Studie?
Die Rechte und Pflichten, die im Zusammenhang mit der Nutzung von IT-Systemen stehen, bilden im Todesfall den digitalen Nachlass eines Menschen. Der digitale Nachlass kann sowohl finanzielle Werte (PayPal-Guthaben, E-Books, ...), als auch ideelle Werte (Facebook-Profil, ...) umfassen. Heute befasst sich kaum ein Mensch mit dem Thema des digitalen Nachlasses. Dies liegt insbesondere daran, dass vielen Menschen nicht bewusst ist, dass und wie sie über ihren digitalen Nachlass verfügen können. Ziel der vorliegenden Studie ist es, das Thema des digitalen Nachlasses in Bezug auf erbrechtliche, datenschutzrechtliche, verbraucherschutzrechtliche und technische Fragestellungen aufzuarbeiten und Empfehlungen für den Umgang mit dem digitalen Nachlass zu geben. Es braucht technische Maßnahmen und rechtliche Vorkehrungen, um den digitalen Nachlass zu regeln und praktisch umzusetzen. Diese Studie untersucht auch, ob gesetzliche Änderungen notwendig sind. Sie umfasst Handlungsempfehlungen für Erblasser und Erben, für Vorsorgebevollmächtigte und Betreuer, für Unternehmen sowie für den Gesetzgeber und die Verwaltung. Schließlich bietet die Studie auch Textvorlagen für die Vorsorgevollmacht und für letztwillige Verfügungen.

Ist der digitale Nachlass vererblich?
Der digitale Nachlass ist gemäß der erbrechtlichen Vorschriften des BGB grundsätzlich vererblich. Erben können vollständig in die Rechtsposition des Erblassers eintreten und alle lokal durch den Verstorbenen gespeicherten Daten einsehen. Sie sind auch berechtigt, Einsicht in die Nutzerkonten des Verstorbenen bei Online-Dienstanbietern zu nehmen und diese weiter zu nutzen. Zudem haben die Erben das Recht, die Konten zu kündigen und zu löschen. Hinsichtlich des erbrechtlichen Übergangs ist dabei aber nach dem jeweiligen Nachlassgegenstand zu differenzieren. So gehen die Daten auf einem lokalen Speichermedium in anderer Weise über als eine Online-Vertragsbeziehung. Die Regelungen des BGB können die Vererbbarkeit dennoch abbilden. Insofern ist nach der hier vertretenen Ansicht keine Anpassung der erbrechtlichen Vorschriften des BGB an etwaige Erfordernisse des digitalen Nachlasses erforderlich. Gegebenenfalls sind jedoch Regelungen anderer gesetzlicher Vorschriften – wie beispielsweise des Urheberrechts – zu beachten.

Woran ist im Rahmen von Betreuung und Vorsorgevollmacht zu denken?
Auch in dem Fall, dass der Verbraucher sich aus gesundheitlichen Gründen nicht mehr selbst um seine Angelegenheiten kümmern kann, können seine digitalen Daten relevant werden.
Ein Nutzer von Online-Diensten kann die Vorsorge treffen, dass im Fall seiner Handlungsunfähigkeit ein Stellvertreter seine digitalen Angelegenheiten regelt. Dabei steht ihm die Möglichkeit offen, selbst einer Person eine Vorsorgevollmacht zu erteilen. Ist dies nicht erfolgt, kann auch ein gerichtlich bestellter Betreuer im Umfang seines Aufgabenkreises für die betroffene Person tätig werden.

Der Stellvertreter ist befugt, auf lokalen Speichermedien des Vertretenen oder auf Servern von Dienstanbietern gespeicherte Daten einzusehen sowie Online-Nutzerkonten des Vertretenen aktiv zu nutzen oder zu kündigen, soweit dies erforderlich ist und von der Ermächtigung gedeckt ist. Dies gilt sowohl für den Betreuer als auch für den Vorsorgebevollmächtigten. Der Betreuer darf dies aber nur, soweit er hierzu durch die gerichtliche Bestellung ermächtigt ist und soweit dies überhaupt für die Durchführung der Betreuung erforderlich ist. Der Vorsorgebevollmächtigte darf dies nur, soweit ihn der Verbraucher selbst durch die Vorsorgevollmacht ermächtigt hat. Hierbei kann in vielen Fällen von einer Rechtmäßigkeit der Datenverarbeitung durch den Stellvertreter ausgegangen werden, allerdings fehlt es bislang noch an ausreichend gefestigter Rechtsprechung, um rechtssichere allgemeingültige Aussagen treffen zu können.

Welche Rechte bestehen an Daten? Ist postmortaler Datenschutz möglich?

Die Forderung nach einem absoluten Recht an Daten erscheint im Kontext des digitalen Nachlasses nicht begründet, da die bestehende Rechtsordnung in ausreichender Weise Zugangs-, Ausschluss- und Verwertungsrechte der Erben gewährleistet.

Postmortaler Datenschutz ist nach dem geltendem Recht möglich. Erblasser können bereits zu Lebzeiten das Verfahren mit den Daten nach dem Tod regeln und auf diese Weise einem ungeregelten Umgang mit dem Nachlass vorbeugen. Diese Möglichkeit entspringt dem zu Lebzeiten bestehenden Recht auf informationelle Selbstbestimmung.

Jede Person genießt zu Lebzeiten Datenschutz. Postmortaler Datenschutz muss dagegen zu Lebzeiten vom Erblasser veranlasst werden und bedarf eine Umsetzung des letzten Willens nach dem Tod. Zur Überwachung der Umsetzung des letzten Willens des Erblassers sollte über externe Kontrollinstanzen nachgedacht werden. Hier bieten sich – soweit die Erben und nächsten Angehörigen nicht personenverschieden sind – beispielsweise die Ernennung eines Testamentsvollstreckers oder eine auf den Tod wirkende Bevollmächtigung an.

Die Erben und nächsten Angehörigen können nach dem Tod des Erblassers ebenfalls für einen Schutz der Daten sorgen. Dies garantiert das postmortale Persönlichkeitsrecht auch dann, wenn der Erblasser keinerlei Regelungen zu Lebzeiten getroffen hat. Der mutmaßliche Wille des Erblassers ist entscheidend, soweit sich ein solcher ermitteln lässt.

Hat der Erblasser keine vorsorglichen Regelungen zu Lebzeiten getroffen, stehen die Daten den Erben im Rahmen des Zugangsanspruches zum Nutzerkonto zur freien Verfügung. Allenfalls die nächsten Angehörigen, soweit sie nicht selbst die Erben sind, könnten überprüfen, ob die Erben den Achtungsanspruch des Erblassers nach seinem Tod wahren. Handeln die Angehörigen und Erben in Personalunion, scheidet eine externe Überwachung der weiteren Verfahrensweise mit den Daten aus. Das Risiko der fehlenden Überprüfbarkeit sowie die Gefahr des Verlusts über die Verfügbarkeit der Daten nach dem Tod verdeutlichen die Relevanz der vorsorglichen Regelung des digitalen Nachlasses.

Welche Handlungsfelder zeigt die Prüfung wichtiger AGB-Klauseln auf?

Dienstanbieter befinden sich gegenüber den Verbrauchern grundsätzlich in einer sehr starken Position. Zum Beispiel geben sie i. d. R. vor, welche Vertragsbedingungen zwischen dem Dienstanbieter und den Verbrauchern – als Dienstnutzer – gelten sollen. Hierfür verwenden Dienstanbieter sogenannte Allgemeine Geschäftsbedingungen (AGB). AGB sind Vertragsbedingungen, die für eine

Vielzahl von Verträgen vorformuliert sind. Wegen des Potenzials, dass Verbraucher durch die Regelungen der AGB und die starke Position der Dienstanbieter benachteiligt werden, muss sich die AGB-Wirksamkeit an den Vorgaben der §§ 305 ff. BGB messen lassen.
Die Untersuchung der AGB der für die vorliegende Studie exemplarisch betrachteten Anbieter PayPal, Microsoft, Apple, Amazon, Sony und Facebook ergab, dass bisher nur wenige Dienstanbieter in den AGB explizit die Vererbbarkeit digitaler Werte regeln. Vorhandene Regelungen betreffen insbesondere die Lizenzierung gekaufter digitaler Werte, die Übertragbarkeit des Nutzerkontos, die Nennung von Nachlasskontakten und die Übertragung von Nutzerkonten und Guthaben auf die Erben.
Die Unterschung der AGB ergab, dass der Schutzumfang, den die §§ 305 ff. BGB bieten, vollständig ist, die Verbraucher jedoch in der Durchsetzung ihrer Ansprüche (besser) unterstützt werden sollten. Dienstanbietern sollten ihre Kunden in allgemeinverständlicher Form über den digitalen Nachlass aufklären. Hierfür könnten sie übersichtliche Symbole und kurze Informationstexte in Form eines „Steckbriefs zum digitalen Nachlass“ verwenden. Zudem könnten unabhängige Institutionen wie Verbraucherschutzverbände die Aufgabe eines Anbietervergleichs übernehmen und ein „(Vergleichs-)Siegel zum digitalen Nachlass“ entwickeln. Das Wort „Kaufen“ sollte in AGB nicht verwendet werden, wenn damit nur der „Erwerb einer lebenslangen Lizenz“ gemeint ist. Benachteiligungen von Erben, die bei dem betreffenden Dienst keine Dienstnutzer sind, müssen vermieden werden. Die AGB sollten den Verbrauchern zu Lebzeiten rechtsverbindliche Wahlmöglichkeiten in Bezug auf ihren digitalen Nachlass einräumen, u. a. die Löschung aller Daten im Todesfall und auch die Möglichkeit, für Nutzerkonten mit verschiedenen digitalen Inhalten auch verschiedene Zugriffsrechte für die Begünstigten zu setzen.

Was sollten Verbraucher beachten?
Die Vorsorge des Verbrauchers kann sich auf die Situation nach seinem Tod oder des Eintritts seiner Handlungsunfähigkeit beziehen. Für die eigene Vorsorge des Verbrauchers hinsichtlich seines digitalen Nachlasses steht ihm grundsätzlich die Möglichkeit der Errichtung eines Testaments zur Verfügung. Hierbei stehen dem Verbraucher verschiedene Regelungsalternativen offen.
So kann der Erblasser beispielsweise einen oder mehrere Erben einsetzen, die das Recht haben, frei über den digitalen Nachlass zu verfügen und die Daten und Nutzerkonten so zu benutzen, wie auch er selbst dies könnte. Möchte der Erblasser bestimmten Personen einen digitalen Inhalt zuwenden, so kann er ein Vermächtnis oder eine Teilungsanordnung in seinem Testament festlegen. Durch eine Auflage kann der Erblasser die Erben anweisen, sich in einer bestimmten Weise zu verhalten. Eine Auflage kann auch bestimmen, dass bestimmte Daten ohne Einsicht gelöscht werden sollen. Für eine weitere Absicherung der Anordnungen kann auch eine Testamentsvollstreckung angeordnet oder eine über den Tod hinaus wirkende Vollmacht erteilt werden. Der Testamentsvollstrecker bzw. Vollmachtnehmer verwaltet dann den Nachlass im Sinne des Erblassers, bis die Nachlassgegenstände unter den Erben aufgeteilt sind. Testamentsvollstreckung und Vollmacht haben verschiedene Vor- und Nachteile. Grundsätzlich hat der Testamentsvollstrecker gegenüber den Erben die stärkere Position, allerdings kann es einige Zeit dauern, bis er durch ein Nachlassgericht in sein Amt berufen wird. Ein Vorsorgebevollmächtigter kann demgegenüber direkt nach dem Tod des Erblassers tätig werden, aber die Erben können ihm die Vollmacht entziehen, sodass er nicht weiter tätig werden darf. Man kann aber beide Möglichkeiten kombinieren.
Möchte der Verbraucher für den Fall vorsorgen, dass er sich alters- oder krankheitsbedingt nicht mehr

selbst um seine Angelegenheiten kümmern kann, bietet sich die Erteilung einer Vorsorgevollmacht an. Dadurch kann einer dritten Person die Befugnis erteilt werden, den Verbraucher für den Fall seiner Handlungsunfähigkeit auch gegenüber Online-Dienstanbietern zu vertreten. Den Umfang dieser Ermächtigung bestimmt der Verbraucher selbst. Dies bietet sich an, wenn verhindert werden soll, dass gerichtlich eine Betreuung angeordnet wird. Daneben kann der Verbraucher aber auch eine Betreuungsverfügung errichten, in der er beispielsweise eine Person benennen kann, die zum Betreuer benannt werden soll.
Daneben sollten Verbraucher getrennt von Testament oder Vorsorgevollmacht den Erben bzw. Vorsorgebevollmächtigten die Namen der genutzten Online-Nutzerkonten mitsamt den Zugangsdaten auflisten und diese Liste stets aktuell halten. Dazu sollten separat auf Papier die Anweisungen, was im Sterbefall mit der Liste zu tun ist (einschließlich Beschreibung des Aufbewahrungsort der Liste) zusammengestellt und zugänglich aufbewahrt werden. Zur Aufbewahrung der Liste kann ein Passwort-Manager oder ein digitaler Datensafes eingesetzt werden, wobei es große Unterschiede zwischen den Produkten gibt. Die meisten dieser Produkte sind Serverlösungen, deren hohe Gebrauchstauglichkeit und Verfügbarkeit mit einer Verminderung von Sicherheit und Datenschutz einhergehen. Der Passwort-Manager KeePass bildet dabei eine Ausnahme, da die Software lokal genutzt wird und unabhängig von einem Anbieter sicher funktioniert. Damit kann die Liste auf einem lokalen Datenträger (z. B. auf einem USB-Stick) gespeichert werden. Die Daten sind mit einem Masterpasswort gesichert, das mit den entsprechenden Anweisungen ausgedruckt und bei einer Vertrauensperson hinterlegt werden kann.
Erben dürfen grundsätzlich Online-Nutzerkonten des Erblassers wie ihre eigenen benutzen, außer in einer letztwilligen Verfügung ist etwas anderes geregelt. Sie dürfen somit die Daten und Nutzerkonten einsehen, aktiv selbst nutzen und Vertragsverhältnisse kündigen. Auch Vorsorgebevollmächtigte und Betreuer haben diese Befugnisse, soweit sie privatautonom bzw. durch ein Gericht hierzu ermächtigt wurden. In beiden Fällen sind aber die Kommunikationspartner des ursprünglichen Nutzers über die Rechtsnachfolge bzw. die Stellvertretersituation zu informieren, indem ein entsprechender Hinweis gegeben wird, um vor allem Irrtümer und Täuschungen im Rechtsverkehr zu vermeiden. Auch der Dienstanbieter ist über den Erbfall bzw. den Beginn der Tätigkeit eines Stellvertreters aufzuklären.
Weiterhin ist die Nutzung eines digitalen Nachlassdienstes zur Vorsorge durch den Erblasser oder ohne Vorsorge im Todesfall durch die Erben möglich. Allerdings sind diese Dienste meist nicht langlebig und werden nicht unbedingt von amtlichen Stellen oder Dienstanbietern akzeptiert. Zudem wird die Sicherheit der hinterlegten Daten bezweifelt. Eine zentrale, staatlich unterstützte Plattform für den Zugriff auf amtliche Dokumente und Nachweise ist denkbar, um die Durchführung des digitalen Nachlasses im Sinne der Verbraucher zu vereinfachen. Allerdings sind viele der damit verbundenen technischen, organisatorischen und rechtlichen Fragen noch ungeklärt. Zudem stehen die mit einer solchen Plattform verbundenen Vorteile im Vergleich zum Aufwand ihrer Errichtung und Verwaltung infrage.

Wie können Erben und Bevollmächtigte ihre Berechtigung nachweisen?
Zudem müssen die Erben und Bevollmächtigten ihre Berechtigung im Rechtsverkehr nachweisen. Dies kann sich insbesondere gegenüber Dienstanbietern mit Sitz im Ausland schwierig darstellen und weitere Probleme bereiten, wenn der Verbraucher bei bestimmten Nutzerkonten ein Pseudonym verwendet hat. Zwar ist es nach hier vertretener Auffassung zumeist – im Rahmen von Vertrags-

verhältnissen mit keinem oder geringem monetären Bezug – ausreichend, wenn den Dienstanbietern lediglich eine Kopie oder ein Scan der Berechtigungsurkunde vorgelegt wird. Allerdings ist dies nichtsdestoweniger davon abhängig, dass die Dienstanbieter diesen Nachweis akzeptieren.
Untersucht wurde daher auch die Frage, ob die erforderlichen Urkunden in digitaler Form vorgelegt werden können, um den Verbrauchern den Nachweis zu erleichtern. Eine originäre digitale Errichtung von letztwilligen Verfügungen und Vorsorgevollmachten ist zwar aufgrund der technischen und rechtlichen Voraussetzungen nicht möglich. Allerdings wird es nach bereits geltender Rechtslage in Zukunft möglich sein, die Beglaubigung erbrechtlicher Urkunden in digitaler Form vorzunehmen, sobald bei den zuständigen Stellen die hierfür erforderliche Infrastruktur vorhanden ist. Eine Anpassung oder Änderung des Zentralen Testamentsregisters ist in diesem Zusammenhang nicht angezeigt. Auch die Ausfertigung von Vorsorgevollmachten in digitaler Form ist technisch bereits möglich. Den hierfür zuständigen Notaren steht zudem bereits die erforderliche Infrastruktur hierfür zur Verfügung. Insofern wären aber Anpassungen des Beurkundungsgesetzes erforderlich, da nach der geltenden Rechtslage die Ausfertigung in digitaler Form noch nicht vorgesehen ist. Eine Erweiterung des Zentralen Vorsorgeregisters ist in diesem Zusammenhang nicht angezeigt. Wird aber das Elektronische Urkundenarchiv zukünftig zu einem Vollmachts- und Titelregister weiterentwickelt, könnte dies auch den Nachweis im Rahmen des digitalen Nachlasses erleichtern.
Daneben müssen Erben und Bevollmächtigte ihre Identität im Rechtsverkehr nachweisen, wenn der Dienstanbieter dies verlangt. Da die persönliche Vorlage von Ausweisen sehr kompliziert sein kann, ist grundsätzlich die Vorlage einer Ausweiskopie (bei Schwärzung der für den Nachweis nicht erforderlichen Stellen) möglich. Dies ist nach hier vertretener Auffassung zumeist ausreichend, ist allerdings davon abhängig, dass die Dienstanbieter diesen Nachweis akzeptieren.
Dagegen bieten vertraglich geregelte Nachweise über den Zugriff auf E-Mail-Konten, Nutzung von digitalen Zertifikaten und Vertrauensdiensten, Telefonnummern, Payment- und Single Sign-On-Verfahren keine sichere oder einfache Alternative. Wird eine starke Identitätsprüfung benötigt, so könnten hierfür neben der persönlichen Legitimationsprüfung vor Ort auch Online-Dienste für die Legitimationsprüfung und die Online-Ausweisfunktion dienen. Diese sind allerdings für beide Seiten aufwendig und zudem faktisch auf Deutschland beschränkt.

Welche vertraglichen Vorsorgemöglichkeiten gibt es?
Eine eigenständige Vorsorge durch den Nutzer kann mit verschiedenen Folgeproblemen verbunden sein, die sich insbesondere im Rahmen der Durchsetzung der Verfügungen gegenüber den Online-Dienstanbietern stellen. Für die Verbraucher ist es daher vorteilhaft, wenn die Dienstanbieter entweder zu individuellen vertraglichen Vereinbarungen mit den Nutzern bereit sind oder vertraglich bestimmte Vorsorgemöglichkeiten zur Verfügung stellen. Eine vertragliche Vorsorge ist sowohl für den Fall des Todes als auch des Eintritts der Handlungsunfähigkeit des Nutzers möglich. Dabei kann der Dienstanbieter dem Verbraucher in einem Formular verschiedene Regelungsalternativen anbieten. Der Dienstanbieter muss dem Verbraucher jedenfalls hinreichend klarmachen, welche Rechtswirkungen die jeweiligen Vereinbarungen haben, und ihm muss offen stehen, ob die Vorsorge durch eine vertragliche Regelung oder durch eigene Vorsorge erfolgen soll. Die vertragliche Vorsorge ist jedenfalls durch entsprechende Konfigurationsmöglichkeiten der Dienste technisch zu unterstützen.
Verschiedene technisch-organisatorische Umsetzungsmöglichkeiten wurden untersucht. Eine Erweiterung der Passwort-Vergessen-Funktion für weitreichende Konfigurationsänderungen würde zusätz-

liche Sicherheitsmaßnahmen erfordern, die aufseiten der Nutzer Kosten verursachen und die Übergabe der Nutzerkonten an Begünstigte komplizierter machen. Die Integration von Social-Media-Plugins (z. B. von Facebook) mit dem Ziel, Begünstigten des digitalen Nachlasses den Zugriff auf das Konto des Erblassers zu gewähren, ist hinsichtlich Datenschutz und Sicherheit fragwürdig. Auch andere Identitätsdienste verlangen, dass Nutzer zunächst ein Nutzerkonto anlegen, wobei in der Regel ebenfalls eine zentrale Datenspeicherung erfolgt.
Konfigurationsmöglichkeiten für den digitalen Nachlass, wie sie Google und Facebook bereits anbieten, haben den Vorteil, dass Nutzer selbstbestimmt den Nachlass regeln können. Allerdings geben die Dienstanbieter die Lösungen vor. Haben die Verbraucher die Kontaktdaten der Begünstigten im Dienst hinterlegt, so können die Dienstanbieter ihnen relativ sicher die Ausübung ihrer Rechte ermöglichen. Solche Konfigurationsmöglichkeiten sind für beide Seiten einfach und preisgünstig, da die Voraussetzungen meist schon erfüllt sind. Eine zweckfremde Nutzung der hinterlegten Kontaktdaten zur Datenerhebung, zur Kundenbefragung oder zur Zusendung von E-Mails mit anderem Inhalt ist den Dienstanbietern vertraglich zu untersagen.

Wie kann der Tod des Erblassers gegenüber den Dienstanbietern nachgewiesen werden?
Der isolierte Nachweis des Todes des Erblassers wird nur im Rahmen einer vertraglichen Regelung zwischen Verbraucher und Dienstanbieter virulent. Liegt keine vertragliche Regelung vor, ist der Todesfall inzident durch Vorlage des Erbscheins oder der eröffneten letztwilligen Verfügung bewiesen.
Die vom Kontoinhaber hinterlegten Kontaktdaten von Vertrauenspersonen können dazu genutzt werden, um nach einer vereinbarten Frist ohne Nutzeraktivität automatische Nachrichten an die Vertrauenspersonen zu senden mit der Bitte, den vermuteten Sterbefall zu bestätigen. Dies sollte allerdings so konfigurierbar sein, dass mehrere Vertrauenspersonen einbezogen werden müssen. Ein bloßes Ausbleiben der Online-Aktivitäten des Erblassers darf für den Dienstanbieter kein hinreichender Grund sein, den Zugriff auf persönliche Daten des Kontoinhabers für andere Personen freizuschalten. Ein Sterbefall muss sicher nachgewiesen werden.
Der Nachweis mittels Sterbeurkunden scheint nahe liegend, ist jedoch nicht trivial, da die Ausstellung und Übermittlung von personenstandsrechtlichen Urkunden noch nicht länderübergreifend harmonisiert sind. Dienstanbieter haben zudem keinen Zugriff auf amtliche Sterberegister, und es ist schwierig, die Echtheit eingescannter Sterbeurkunden zu prüfen. Eine öffentliche Blockchain, um Sterbeurkunden international verfügbarer und leichter überprüfbar zu machen, wäre theoretisch denkbar. Da es sich aber um besonders sensible Daten handelt, müssen besondere Sicherheitsanforderungen gelten, die durch eine Blockchain kaum erfüllt werden können.
Ob und in welcher Form eine Sterbeurkunde gegenüber einem Dienstanbieter vorgelegt werden muss, kann vertraglich geregelt werden. So kann im Rahmen der vertraglichen Regelung die Vorlage einer Kopie oder eines Scans der (deutschen) Sterbeurkunde für ausreichend erklärt werden.

Was sollten Unternehmen beachten?
Dienstanbietern wird u. a. empfohlen, ihre Dienstnutzer in angemessener – d. h. in kurzer und allgemeinverständlicher – Form über deren Rechte in Bezug auf das digitale Erbe aufzuklären. Insbesondere Anbietern sozialer Netzwerkplattformen kann darüber hinaus empfohlen werden, ihren Dienstnutzern über die AGB eine Wahlmöglichkeit in Bezug auf deren digitalen Nachlass einzuräumen, sodass sie z. B. zu Lebzeiten wählen können, dass ihr Account in ihrem Todesfall gelöscht werden

soll, ohne dass Erben (vorher) Zugriff auf diesen erhalten. Das Einräumen einer Wahlmöglichkeit zum digitalen Nachlass über die AGB des Dienstanbieters sollte zusätzlich technisch durch Konfigurationsmöglichkeiten des Nutzerkontos unterstützt werden, um den Verbraucher in die Lage zu versetzen, aus den verschiedenen Nachlassoptionen die gewünschte Option für sein Nutzerkonto festzulegen. Neben der Löschung des gesamten Nutzerkontos wären die Archivierung der Daten zur Ansicht und die vollständige Übergabe des Nutzerkontos an die Erben sinnvolle Optionen. Für verschiedene Daten des Nutzerkontos sollte ein unterschiedlicher Umgang im digitalen Nachlass festgelegt werden können, beispielsweise, dass die Erben Zugriff auf sämtliche Fotos, nicht aber auf sonstige Beiträge erhalten sollen, oder dass E-Mails zwar angesehen, aber nicht mehr neu im Namen des Erblassers geschrieben werden dürfen. Die Konfiguration des Nutzerkontos sollte aber auch zulassen, dass der Nutzer sich an dieser Stelle auf keine Regelung festlegt.

Was müssen Gesetzgeber und Verwaltung beachten?

Zur Erleichterung der Vorsorge von Erblassern könnte das Zentrale Testamentsregister um die Möglichkeit erweitert werden, in diesem auch (notarielle) Vorsorgeurkunden zu registrieren. Um den Nachweis der Legitimation eines Vorsorgebevollmächtigten im Rechtsverkehr zu erleichtern, könnte im Beurkundungsgesetz die Möglichkeit geschaffen werden, dass Notare Ausfertigungen von Urkunden auch in elektronischer Form erteilen können. Alternativ wäre es auch aus Sicht des digitalen Bereichs sinnvoll, das Elektronische Urkundenarchiv zu einem Vollmachts- und Titelregister weiterzuentwickeln.

Der Schutzumfang, den die §§ 305 ff. BGB in Bezug auf die wirksame Einbeziehung und die Wirksamkeit von AGB für Verbraucher vorsehen, scheint vollständig. Änderungsbedarf an den §§ 305 ff. BGB ergibt sich daher nicht. Jedoch sollte die Diskussion um die Rechtsdurchsetzung von Ansprüchen der Verbraucher fortgesetzt werden.

Da Erblassern derzeit häufig weder bewusst ist, was mit ihren persönlichen Daten und finanziellen, digitalen Werten nach ihrem Tod passieren wird, noch ihnen bewusst ist, dass sie darauf aktiv Einfluss nehmen können, ist zudem zu empfehlen, Verbraucher im Rahmen von Awarenesskampagnen auch in Zukunft für das Thema des digitalen Nachlasses zu sensibilisieren.

Eine Sensibilisierung der Verbraucher kann auch durch eine gesetzlich geregelte Informationsverpflichtung der Dienstanbieter erreicht werden. Empfohlen wird eine gesetzliche Informationspflicht für Dienstanbieter hinsichtlich einer Verarbeitung von personenbezogenen Daten nach dem Tod. Den Verbrauchern sollte auf diesem Wege transparent dargelegt werden, dass die zu Lebzeiten verarbeiteten, personenbezogenen Daten mit dem Tod nicht einfach gelöscht oder auf sonstige Weise entfernt werden. Die gesetzliche Informationspflicht soll sich aus drei Elementen zusammensetzen: Dienstanbieter sollten im Rahmen ihrer AGBs mindestens (1) einen Hinweis auf den grundsätzlichen Übergang des Nutzerkontos und der darin enthaltenen Daten auf die Erben geben. (2) Weiterhin sollten die Dienstanbieter verpflichtet werden, dem Verbraucher als Nutzer des Online-Dienstes eine oder mehrere Wahlmöglichkeiten hinsichtlich der Regelung des Verfahrens mit den Daten nach dem Tod zur Verfügung zu stellen. Schließlich (3) bedarf es eines Hinweises auf die Möglichkeit, eine detailliertere und weitergehende Vorsorge im Rahmen einer letztwilligen Verfügung oder einer Bevollmächtigung auf den Tod zu treffen.

Definitionen

Absolutes Recht Ein Recht, das gegenüber jedermann wirkt.

Allgemeine Geschäftsbedingungen (AGB) Dies sind im Unterschied zu einer Individualabrede alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen.

Bestellungsurkunde Ein Betreuer erhält eine Urkunde über seine Bestellung (§ 290 FamFG). Darin enthalten sind u.a. die Bezeichnung des Betroffenen und des Betreuers und der Aufgabenkreis des Betreuers.

Betreuung Dies meint die gesetzliche Vertretung von Volljährigen, die für ihre eigenen Angelegenheiten alters- oder krankheitsbedingt nicht oder nicht ausreichend sorgen können. Betreuer obliegen zahlreiche Pflichten gegenüber dem Betreuten und dem Betreuungsgericht.

Betreuungsverfügung Dies ist eine Möglichkeit der persönlichen und selbstbestimmten Vorsorge für den Fall, dass jemand selbst nicht mehr in der Lage ist, seine eigenen Angelegenheiten zu erledigen. Ihr Vorteil ist, dass sie nur dann Wirkungen entfaltet, wenn es tatsächlich erforderlich wird (§ 1896 BGB).

Bevollmächtigung Darunter versteht man die durch ein Rechtsgeschäft begründete Vertretungsmacht.

Blockchain Dies ist eine kontinuierlich erweiterbare Liste von Datensätzen, „Blöcke“ genannt, die mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptografisch sicheren Hashwert des vorhergehenden Blocks, einen Zeitstempel und die eigentlichen Transaktionsdaten.

Cloud Computing Dies ist eine IT-Infrastruktur, die meist über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung.

Datenschutz-Grundverordnung (DSGVO) Die Datenschutz-Grundverordnung ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten sichergestellt und andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Deliktsrechtlicher Schutz Gesetzlicher Schutz vor schädigenden Handlungen, die imstande sind, Rechtsgüter des Einzelnen zu verletzen.

Dienstanbieter Synonyme: *Anbieter*, *Provider*. Dies sind Anbieter von Diensten, Inhalten oder technischen Leistungen für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet.

Digitaler Nachlass Dies umfasst die Rechtspositionen eines verstorbenen Internetnutzers, insbesondere dessen Vertragsbeziehungen zu Dienstanbietern von E-Mails, sozialen Netzwerken oder virtuellen Konten. Es zählen auch Eigentumsrechte des Verstorbenen an Hardware, Nutzungsrechte an der Software, Urheberrechte und Rechte an hinterlegten Bildern, Foreneinträgen und Blogs dazu.

Digitale Rechteverwaltung Engl.: *Digital Rights Management*. Dies bezeichnet Verfahren, mit denen die Nutzung (und Verbreitung) digitaler Medien kontrolliert werden soll.

Digitale Signatur Dies bezeichnet meist Verfahren auf Basis von kryptografischen Schlüsseln. Dabei berechnet der Signaturersteller zu einer digitalen Nachricht mithilfe eines geheimen Signaturschlüssels einen Wert, der ebenfalls digitale Signatur genannt wird. Dieser Wert ermöglicht es jedem, mithilfe des zugehörigen öffentlichen Signaturprüfschlüssels die Urheberschaft und Integrität der Nachricht zu prüfen. Die digitale Signatur ist ein technischer Begriff, während die elektronische Signatur (siehe unten) eher ein juristischer Begriff ist.

Digitales Zertifikat Dies ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Die Ausstellung des Zertifikats erfolgt oft durch eine offizielle Zertifizierungsstelle.

Elektronische Signatur Dies sind mit digitalen Dokumenten verknüpfte Daten, mit denen man den Unterzeichner identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann. Die sogenannte fortgeschrittene elektronische Signatur kann eindeutig dem Unterzeichner zugeordnet werden und ermöglicht es, den Unterzeichner zu identifizieren. Eine fortgeschrittene elektronische Signatur, die auf einem Zertifikat einer entsprechend akkreditierten Zertifizierungsstelle beruht und mit einer sicheren, hardwarebasierten Signaturerstellungseinheit (z. B. Signaturkarte) erstellt wurde, wird als qualifizierte elektronische Signatur bezeichnet. Diese erfüllt denselben Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten, weshalb sie die Schriftform regelmäßig auch ersetzen kann.

Erbe Erbe oder Nachlassempfänger ist diejenige Person, auf die im Falle des Versterbens einer anderen Person (Erbfall) deren Vermögen (Erbschaft, Nachlass) übergeht.

Erblasser Der Erbfall tritt mit dem Tod einer natürlichen Person, des Erblassers, ein. Der Erblasser ist diejenige Person, um deren Nachfolge von Todes wegen es geht. Mit dem Erbfall geht das gesamte Vermögen des Erblassers auf den oder die Erben über (§ 1922 I BGB).

Erbvertrag Ein Erbvertrag ist gleichzeitig ein Vertrag und eine Verfügung von Todes wegen. Dies bietet neben dem Testament eine zweite Möglichkeit, durch Verfügung von Todes wegen Regelungen über den Verbleib des eigenen oder gemeinschaftlichen Vermögens nach dem Tod zu treffen und von der gesetzlichen Erbfolge abzuweichen (§ 1941 und §§ 2274 ff. BGB). Ein Erbvertrag kann nur von volljährigen Personen und nur gegenüber einem Notar abgeschlossen

werden. Der wesentliche Unterschied zum Testament besteht darin, dass der Erblasser sich beim Erbvertrag gegenüber einem Vertragspartner bindet.

Ersatzerbschaft Das ist ein Erbe, der dann zum Zug kommt, wenn der eingesetzte Erbe nicht erben kann (z. B. schon gestorben ist) oder nicht erben will und daher die Erbschaft ausschlägt. Nimmt der eingesetzte Erbe die Erbschaft an, erlischt die Ersatzerbschaft. Eine Ersatzerbschaft kann bei der Abfassung eines Testaments vorgesehen werden, d. h. es kann ein Ersatzerbe benannt werden.

Erschöpfungsgrundsatz Dies ist ein Rechtsgrundsatz aus dem Immaterialgüterrecht. Schutzrechte, die der Erschöpfung unterliegen, „verbrauchen“ sich, in der Regel sobald der geschützte Gegenstand zum ersten Mal rechtmäßig in Verkehr gebracht wurde. Der Schutz kann danach nicht mehr in Anspruch genommen werden. Bezugsobjekt des Erschöpfungsgrundsatzes ist immer ein konkreter Gegenstand.

Formvorschrift Von der einfachsten bis zur strengsten Form: Die *Textform* (§ 126b BGB) meint eine Urkunde oder ein ein anderes Dokument, das zur dauerhaften Wiedergabe in Schriftzeichen geeignet ist. Die *Elektronische Form* (§ 126a BGB) muss den Aussteller enthalten und mit einer qualifizierten elektronischen Signatur versehen sein. Die *Schriftform* (§ 126 BGB) meint Schriftstücke, Verträge oder Urkunden, die vom Aussteller und dessen Vertragspartner eigenhändig unterzeichnet sind. Die *Beglaubigung* (§ 129 BGB) meint eine schriftliche Erklärung, die vom Erklärenden unterschrieben und von einem Notar beglaubigt ist. Die *Beurkundung* (§ 128 BGB) muss von einem Notar in einer Niederschrift abgefasst, von diesem den Beteiligten vorgelesen, von den Beteiligten genehmigt und in Anwesenheit des Notars eigenhändig unterzeichnet werden.

Fürsorgebedürfnis Das Hilfs- oder Fürsorgebedürfnis ist Voraussetzung für die Anordnung einer Betreuung. Ein Betreuer darf nur bestellt werden, wenn die betroffene Person sich aufgrund einer Krankheit oder Behinderung ganz oder teilweise nicht mehr selbst um ihre Angelegenheiten kümmern kann und sie daher der Hilfe eines Betreuers bedarf.

Gebrauchstauglichkeit Englisch: *usability*. Dies bezeichnet das Ausmaß, in dem ein Produkt, System oder ein Dienst durch bestimmte Nutzer in einem bestimmten Anwendungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen. Sie ist damit eng verwandt mit dem breiter gefassten Konzept der User Experience.

Gewillkürter Stellvertreter Bei der gewillkürten Stellvertretung beruht die Vertretungmacht des Stellvertreters nicht auf dem Gesetz, sondern auf einem Rechtsgeschäft (z. B. einer Vollmacht). Der Vollmachtgeber könnte auch selbst handeln, bestellt aber einen Stellvertreter, der Rechtsgeschäfte für ihn abschließen darf.

Immaterialgüterrecht Dies bezeichnet ein ausschließliches Recht an einem immateriellen Gut, etwa einem Kunstwerk oder einer technischen Erfindung, im Unterschied zum Eigentum an körperlichen Gegenständen (Sachen im Sinne des § 90 BGB).

Kryptografischer Hashwert Ergebnis einer Hashfunktion, die effizient eine Zeichenfolge beliebiger Länge (Eingabewert) auf eine Zeichenfolge mit fester Länge (Hashwert) abbildet. Hashwerte dienen vor allem zur Integritätsprüfung von Dateien oder Nachrichten und als Eingabe bei der Erstellung von elektronischen Signaturen.

Kryptografischer Schlüssel Digitale Daten, die in einem Verschlüsselungsverfahren eingesetzt werden, um die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit von Informationen zu schützen.

Kryptowährung Dies sind digitale Zahlungsmittel, die auf kryptografischen Werkzeugen wie Blockchains und digitalen Signaturen basieren. Als Zahlungssystem sollen sie unabhängig, verteilt und sicher sein. Sie sind keine Währungen im eigentlichen Sinne. 2009 wurde mit dem Bitcoin die erste Kryptowährung öffentlich gehandelt. Inzwischen gibt es Tausende von Kryptowährungen.

Kundgabe Durch besondere Mitteilung an einen Dritten oder öffentliche Bekanntmachung kann ein Vollmachtgeber bekanntgeben, dass er einen anderen bevollmächtigt hat (§ 171 BGB). Dies hat zur Folge, dass der Vollmachtnehmer im ersten Fall gegenüber dem Dritten, im zweiten Fall jedem Dritten gegenüber zur Stellvertretung auch dann ermächtigt ist, wenn gar keine Vollmacht mehr besteht. Es entsteht ein Rechtsschein der Vollmacht.

Legitimationsklausel Eine AGB-Klausel, die eine bestimmte Art des Nachweises für die Erbenstellung vorsieht.

Leistungstreuepflicht Die Leistungstreuepflicht ist eine der Rücksichtnahmepflichten im Vertragsverhältnis. Die Vertragsparteien haben dabei alles zu unterlassen, was den Zweck des Vertrages oder den Leistungserfolg gefährden oder beeinträchtigen könnte, sowie alles Zumutbare zu tun, um den Erfolg zu ermöglichen.

Masterpasswort Zur Verschlüsselung von mehreren gespeicherten Passwörtern und anderen Zugangsdaten – beispielsweise in einem Passwort-Manager oder Webbrowser – genutztes Hauptkennwort, das vom Nutzer eingegeben werden muss, um die einzelnen Zugangsdaten nutzen zu können. Da oftmals allein das Masterpasswort den Zugriff zu vielen Diensten ermöglicht, muss es besonders gut geschützt werden.

Musterfeststellungsklage Dies ist eine zivilrechtliche Verbandsklage, die mit dem Gesetz zur Einführung einer zivilprozessualen Musterfeststellungsklage mit Wirkung zum 1. November 2018 in das deutsche Recht eingeführt wurde. Klageberechtigt sind ausgewählte Verbände.

Nacherbschaft Nacherbe ist, wer in der Weise zum Erben eingesetzt wird, dass er erst Erbe wird, nachdem zunächst ein anderer Erbe geworden ist. Nacherbe wird also nur, wer durch eine Verfügung von Todes wegen dazu bestimmt wird. Für den Eintritt der Nacherbschaft können verschiedene Bedingungen bestimmt werden (z. B. Tod des Vorerben, Volljährigkeit des Nacherben).

Nachlassdienst Dies ist eine Dienstleistung, die dabei hilft, einen Nachlass zu regeln und ihn den Erben zu übergeben. Dazu gehören z. B. Vertragsaktualisierungen wie Abmeldungen und Ummeldungen bei Institutionen, Organisationen, Unternehmen und Dienstanbietern einschließlich der Vorsorge und Nachsorge des digitalen Nachlasses.

Nutzerkonto Synonyme: *Account*, *Konto*. Ein Nutzerkonto ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Üblicherweise muss ein Benutzer sich beim Einloggen mit Benutzernamen und Kennwort ausweisen. Zusammen mit dem Nutzerkonto werden in der Regel persönliche Daten, Konfigurationseinstellungen und ggf. auch digitale Werte des jeweiligen Nutzers gespeichert.

Online-Ausweisfunktion Dies ist eine Funktion des Personalausweises, mit der die Ausweisinhaber ihre Identität im Internet sicher nachweisen können. Vor der Datenübermittlung sieht der Nutzer, welches Unternehmen bzw. welche Behörde seine Daten erhält und ob die für die Datenabfrage erforderliche staatliche Berechtigung dafür vorliegt.

Online-Dienst Dies ist eine Dienstleistung, die über das Internet genutzt werden kann. Der Dienstanbieter stellt die benötigte serverseitige Infrastruktur zur Verfügung. Der Nutzer nutzt einen entsprechenden Client (ein Gerät bzw. eine Software), über den die Inhalte ausgegeben werden. Die meisten Online-Dienste sind Webanwendungen, die über einen Webbrowser benutzt werden können.

Postident Dies bezeichnet verschiedene Verfahren der persönlichen Identifikation von Personen, die durch die Mitarbeiter der Deutschen Post AG vorgenommen werden. Man spricht bei Postident-Verfahren auch von einer unpersönlichen Legitimationsprüfung. Die Verfahren können z. B. zur Zusendung von Unterlagen an einen Vertragspartner inklusive Unterzeichnung eines Dokuments dienen.

Postmortale Vollmacht Die Vollmacht entfaltet erst mit dem Tod des Vollmachtgebers ihre Wirkung. Erst mit dem Eintritt des Todes des Vollmachtgebers ist der Vollmachtnehmer zur Stellvertretung ermächtigt.

Postmortaler Datenschutz Nach dem Tod eines Menschen, ist die DSGVO nicht mehr anwendbar. Unter postmortalem Datenschutz sind daher alle Maßnahmen, Ansprüche und Rechte zu verstehen, die den Schutz von solchen Daten gewährleisten, die zwar nicht mehr unter das Regelungsregime des Datenschutzrechts fallen, gleichwohl aber schutzbedürftig sind.

Postmortales Persönlichkeitsrecht Das postmortale Persönlichkeitsrecht (abgeleitet aus Art. 1 I GG) ist die Grundlage für einen Schutz von Daten nach dem Tod. Geschützt ist bei Verstorbenen grundsätzlich der allgemeine Achtungsanspruch, der auch nach dem Tod fortwirkt und dem Menschen kraft seines Personenseins zusteht.

Rechtsschein Dies bedeutet, dass nicht wirklich ein Recht besteht, sondern nur der äußere Anschein eines in Wahrheit nicht bestehenden Rechts. Ausnahmsweise wird aber derjenige geschützt, der im guten Glauben an das Bestehen des Rechts handelt. Dies ist beispielsweise der

Fall, wenn durch eine Person zurechenbar der Anschein erweckt wurde, dass eine dritte Person sie vertreten darf.

Single Sign-On (SSO) Dies bedeutet, dass ein Nutzer nach einem einmaligen Login bei einem Dienst auch auf andere Dienste zugreifen kann, ohne sich an den einzelnen Diensten zusätzlich anmelden zu müssen. Ziel des Single Sign-On ist es, dass sich der Benutzer nur einmal unter Zuhilfenahme eines einzigen Nutzerkontos identifizieren muss. Danach übernimmt das SSO-System die Aufgabe, die erkannte Identität gegenüber den anderen Diensten zu bestätigen.

Social Media Dies ist ein Oberbegriff für digitale Medien und Methoden, die es Nutzern ermöglichen, sich im Internet zu vernetzen, um sich untereinander auszutauschen und mediale Inhalte einzeln oder in einer definierten Gemeinschaft oder offen in der Gesellschaft zu erstellen und weiterzugeben. Kategorien von Social Media sind beispielsweise: Öffentliche und unternehmensinterne soziale Netzwerke, Blogs, berufliche Netzwerke, Foren, Mikroblogs, Foto-Sharing, Produkt-/Service-Reviews, Social Bookmarks, soziale Spiele, Videoportale und virtuelle Welten.

Soziales Netzwerk Dies ist ein Online-Dienst, der es Nutzern ermöglicht, Informationen auszutauschen, Beziehungen zu anderen Nutzern aufzubauen und zu pflegen. Zum wechselseitigen Austausch von Meinungen, Erfahrungen und Informationen wird eine Social Media Kommunikationsplattform eingesetzt. Eine dadurch entstehende Online-Community kommuniziert entsprechend der Möglichkeiten der jeweiligen Plattform im virtuellen Raum.

Stellvertretung Handeln einer Person innerhalb der ihr zustehenden Vertretungsmacht im Namen des Vertretenen (§ 164 BGB).

Sterbeurkunde In die Sterbeurkunde werden u. a. aufgenommen: die Vornamen und der Familienname des Verstorbenen, Ort und Tag seiner Geburt sowie seine rechtliche Zugehörigkeit zu einer Religionsgemeinschaft, sofern sich die Zugehörigkeit aus dem Registereintrag ergibt, der letzte Wohnsitz und der Familienstand des Verstorbenen sowie Sterbeort und Zeitpunkt des Todes (§ 60 PStG).

Teilungsanordnung Eine Teilungsanordnung kann nach § 2048 BGB vom Erblasser im Testament verfügt werden, wenn mehrere Personen Erben werden. Mit der Anordnung wird geregelt, wie ein oder mehrere Nachlassgegenstände bei der Auseinandersetzung unter den Miterben verteilt werden sollen.

Testament (oder auch letztwillige Verfügung) Dies ist eine Form der Verfügung von Todes wegen, eine Regelung für den Erbfall und wird auch als letztwillige Verfügung bezeichnet (§ 1937 BGB). Sie ist eine einseitige, formbedürftige, jederzeit widerrufbare Willenserklärung des Erblassers dahingehend, was im Fall seines Todes mit seinem Vermögen geschehen soll. Eine andere Form der Verfügung von Todes wegen ist der Erbvertrag (§§ 1941, 2274 ff. BGB).

Testamentsvollstreckung Vollziehung des letzten Willens eines Erblassers durch eine in der Regel vom Erblasser ernannte Person (§§ 2197 ff. BGB).

Totalbetreuung Dies bedeutet, dass der Betreuer nicht nur für einzelne, sondern zur Besorgung aller Angelegenheiten der betroffenen Person bestellt wird. Der Betreuer kann die betroffene Person in allen Bereichen rechtlich unterstützen und vertreten. Dies ist aber eher die Ausnahme.

Transmortale Vollmacht Der Stellvertreter verliert nicht mit dem Tod des Vollmachtgebers seine bereits bestehende Vertretungsmacht, sondern die Vollmacht wirkt über den Tod des Vollmachtgebers hinaus.

Transparenzgebot Dies entspricht dem Transparenzprinzip, demgemäß die allgemeine Geschäftsbedingungen (AGB) so formuliert sein müssen, dass sich die Rechte und Pflichten des Vertragspartners klar daraus ergeben.

Universalsukzession Mit dem Tod einer Person geht deren Vermögen kraft Gesetzes als Ganzes unmittelbar und von selbst auf eine oder mehrere andere Personen (Erben) über (§ 1922 BGB).

Vererbbarkeit Das gesamte Vermögen des Erblassers geht im Wege des Erbrechts auf die Erben über, nicht aber die höchstpersönlichen Rechte des Erblassers.

Verfügung von Todes wegen Dies ist eine Anordnung, die eine oder mehrere natürliche Personen für den Fall ihres Todes treffen und erst mit dessen Eintritt wirksam werden soll. Darin wird die Übertragung des Vermögens des Erblassers auf seine Erben geregelt (z. B. durch Testament).

Vermächtnis Ein erbrechtliches Vermächtnis ist die Zuwendung eines bestimmten Vermögensvorteils aufgrund eines Testaments oder Erbvertrags, ohne dass der mit dem Vermächtnis Bedachte (der Vermächtnisnehmer) als Erbe eingesetzt wird.

Vertrauensdienst Dies bezeichnet verschiedene Dienste nach der eIDAS-Verordnung in den Bereichen elektronische Signaturen, Siegel, Zeitstempel, Einschreiben und digitale Zertifikate. eIDAS steht für „electronic IDentification, Authentication and trust Services. Die Verordnung regelt die elektronische Identifizierung und die Vertrauensdienste für elektronische Transaktionen im europäischen Binnenmarkt.

Vollmacht Dies ist die durch ein Rechtsgeschäft begründete Vertretungsmacht. Der Besitzer einer Vollmacht ist Bevollmächtigter (auch Vollmachtnehmer). Eine Generalvollmacht ermächtigt zum Abschluss aller vertretungszulässigen Rechtsgeschäfte, die Einzelvollmacht hingegen nur zur Vornahme einer einzelnen, genau bestimmten Handlung. Die Vorsorgevollmacht regelt den Fall der möglicherweise später eintretenden Geschäftsunfähigkeit. Es gibt Vollmachten, die nur bis zum Tod gelten (prämortale Vollmacht), auch nach dem Tod des Vollmachtgebers gelten (transmortale Vollmacht), oder nur nach dem Tod gelten (postmortale Vollmacht).

Vorausvermächtnis Dies ist ein Vermächtnis, das einem (Mit-)Erben selbst zugewendet wird, d. h. dieser ist sowohl Erbe als auch Vermächtnisnehmer (§ 2150 BGB). Er erhält einen bestimmten Gegenstand aus dem Nachlass im Voraus und ohne Anrechnung auf seinen Erbteil. In der Praxis von der Teilungsanordnung abzugrenzen.

Vorerbschaft Der Vorerbe ist wahrer Erbe, allerdings bestimmt der Erblasser, dass ihm eine andere Person auf eine bestimmte Bedingung hin zeitlich nachfolgen soll (Nacherbe). Der Vorerbe unterliegt gewissen Beschränkungen.

Vorsorgevollmacht Damit bevollmächtigt eine Person eine andere Person, im Falle einer Notsituation alle oder bestimmte Aufgaben für den Vollmachtgeber zu erledigen. Mit der Vorsorgevollmacht wird der Bevollmächtigte zum Vertreter im Willen, d. h. er entscheidet anstelle des nicht mehr entscheidungsfähigen Vollmachtgebers.

Zwei-Faktor-Authentisierung Dies bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden, oder Passwort und TAN beim Onlinebanking.

1 Der digitale Nachlass: Eine Einführung

Dieses Kapitel

- stellt die Motivation vor, die zur Umsetzung der vorliegenden Studie geführt hat,
- stellt die Zielsetzung und -gruppen der vorliegenden Studie vor,
- definiert den Begriff des digitalen Nachlasses,
- nennt Beispiele für ideelle und finanzielle Werte des digitalen Nachlasses,
- gibt einen Überblick über relevante Vorarbeiten zum Thema.

1.1 Motivation, Zielsetzung und Zielgruppen dieser Studie

Obwohl sich ein jeder Mensch in seinem Leben zwangsläufig mit den Themen des Erbens und Vererbens beschäftigen muss, ist nur wenigen Menschen bewusst, dass das Erbe auch aus digitalen Werten – dem sogenannten „digitalen Nachlass“ bestehen kann. Selbst Menschen, die sich dieser Tatsache bewusst sind, treffen i. d. R. keinerlei Vorkehrungen für ihre digitalen Werte, obwohl dies aus Sicht des Erblassers – also aus Sicht des Menschen, der Vorsorge für seinen Todesfall treffen möchte – dringend anzuraten ist.

Dies lässt sich aus heutiger Sicht insbesondere damit begründen, dass den Wenigsten bewusst ist

- was (ohne ihr vorheriges Einwirken) nach ihrem Tod mit ihrem digitalen Nachlass passieren wird,
- wie sie ihren digitalen Nachlass praktisch vorbereiten und umsetzen können und
- wie sie und ihre Erben durch technische Lösungen bei der Umsetzung und Durchsetzung des digitalen Nachlasses unterstützt werden können.

Der letztgenannte Aspekt deutet bereits ein weiteres Problemfeld des digitalen Nachlasses an: Selbst wenn den *Erben* der (potenzielle) Wert eines digitalen Nachlasses bewusst wäre, ist es für diese extrem aufwendig, teilweise schier unmöglich, sämtliche Werte des digitalen Nachlasses nach dem Tod des Erblassers aufzuspüren. Dies liegt nicht zuletzt an der Masse unterschiedlicher Online-Dienste und Online-Dienstanbieter, bei denen potenzielle Werte des Erblassers vorliegen könnten, sowie an dem Umstand, dass einige dieser Dienste durch den Erblasser womöglich unter einem Pseudonym genutzt wurden und für die Erben daher das Auffinden eines Accounts zusätzlich erschwert werden kann.

Vor diesem Hintergrund hat sich die vorliegende Studie zum Ziel gesetzt, das Thema des digitalen Nachlasses aufzuarbeiten. Im Fokus stehen hierbei erbrechtliche, datenschutzrechtliche, verbraucherschutzrechtliche und technische Fragestellungen. Es wurden u. a. herausgearbeitet,

- welche Rechte dem Erblasser zustehen,
- welche Möglichkeiten für den Erblasser bestehen, seinen digitalen Nachlass zu regeln,
- welche Schwierigkeiten und Benachteiligungen in diesem Zusammenhang auf Verbraucher zukommen können und
- wie durch (technische) Maßnahmen und (rechtliche) Vorkehrungen die Ausgangslage der Erben nach dem Ableben des Erblassers verbessert werden kann.

Neben der Darstellung der rechtlichen und technischen Aspekte rund um das Thema „digitaler Nachlass“ zeigt die Studie Möglichkeiten auf, durch die die aktuelle Situation zum digitalen Nachlass aus Sicht verschiedener Zielgruppen verbessert werden könnte. Im Fokus solcher Empfehlungen stehen hierbei zunächst der Erblasser und die Erben selbst. Doch auch die Situationen, in denen ideelle und

finanzielle digitale Werte zu Lebzeiten von Dritten verwaltet werden müssen, soll nicht unberücksichtigt bleiben, sodass sich die Studie mit Empfehlungen auch an Vorsorgebevollmächtigte und Betreuer wenden möchte. Auch sind (kleine und mittelständische) Unternehmen sowie der Gesetzgeber und die Verwaltung Adressaten möglicher Empfehlungen. Zum einen wird aufgezeigt, wie Unternehmen als Anbieter von Online-Diensten die Situation ihrer Kunden rund um deren digitalen Nachlass im jeweilig genutzten Dienst verbessern können. Zum anderen wird diskutiert, ob ggf. Gesetzesänderungen oder -ergänzungen die aktuelle Situation von Erben, Erblassern, Vorsorgebevollmächtigten und Betreuern verbessern können.

1.2 Definition des digitalen Nachlasses

Erblasser hinterlassen im Sterbefall zunehmend elektronische Daten, Vertragsbeziehungen mit Telekommunikationsanbietern und Internetdienstleistungen und vieles andere in digitaler Form. Der digitale Nachlass lässt sich als die „Gesamtheit des digitalen Vermögens“ definieren. Dazu gehören alle Rechtsverhältnisse, Rechte und Pflichten des Erblassers im Zusammenhang mit IT-Systemen und die damit verbundenen elektronischen Daten – also sämtliche gespeicherten Daten auf lokalen Datenträgern, im Internet und in Cloud-basierten Diensten, alle Nutzerkonten und Zugangsdaten.[1] Auch die vom Erblasser elektronisch verfassten und im Internet gespeicherten Texte (z. B. E-Mails, Beiträge in sozialen Netzwerken und Blogs), Fotos, Videos und Audio-Aufnahmen gehören gemäß Urheberrechtsgesetz zum digitalen Nachlass. Nicht nur die eigenen digitalen Inhalte sind relevant, sondern auch die Plattformen, auf denen die Inhalte gespeichert und mit anderen Nutzern geteilt werden, einschließlich personenbezogener Profildaten und der Spuren (Metadaten, Logdaten), die die Nutzer hinterlassen, wenn sie sich im Internet bewegen und kommunizieren.[2] Selbst diese kommunikativen Spuren sind soziale monetarisierbare Daten, die in aggregierter Form für Werbetreibende und Unternehmen interessant sein können.[3]

Zu den persönlichen digitalen Werten können beispielsweise zählen:

- In sozialen Netzwerken (Facebook, Twitter, Instagram, Vimeo, Soundcloud, ...) hinterlassene Daten.
- Persönliche Konten mit eigenen Daten (z. B. Blogs, Urheberrechte, Rechte an Webseiten und Domainnamen, eigener Online-Handel, YouTube-Accounts mit Werbeeinnahmen).
- Digitale Inhalte in Form von elektronischen Büchern und heruntergeladenen Musikdateien.
- Mit Spielkonten verbundene Werte wie virtuelle Spielfiguren, Grundstücke und Guthaben.
- Im elektronischen Handel und bei elektronischen Buchungen erworbene Bonuspunkte und Rabatte (z. B. Flugmeilen).

[1] *Funk*, Das Erbe im Netz: Rechtslage und Praxis des digitalen Nachlasses, S. 3.
[2] *Brucker-Kley u. a.*, Passing and passing on in the digital world – Issues and solutions for the digital estate, in: IADIS 2013, S. 36.
[3] *Kneese*, Networked heirlooms: the affective and financial logics of digital estate planning, in: Cultural Studies 33.2, S. 19.

- Virtuelles Geld und Geldbörsen mit Guthaben auf elektronischen Plattformen (Bitcoins, Guthaben bei PayPal).
- Bestehende kostenpflichtige Vertragsbeziehungen mit Online-Dienstanbietern.

In der Regel handelt es sich bei den persönlichen Daten wie Blog-Einträgen, Twitter-Posts und Urlaubsbildern um ideelle Werte des digitalen Nachlasses,[4] während elektronische Bücher und Musikdateien, virtuelle Spielstände und virtuelles Geld finanzielle Werte des digitalen Nachlasses darstellen.

1.3 Vorhandene Arbeiten

Das Thema „digitaler Nachlass“ ist bisher nur geringfügig in der Literatur vertreten. Neben vereinzelten Fachartikeln und Monografien, die in der vorliegenden Studie an den jeweils relevanten Stellen Erwähnung finden, sind insbesondere folgende Arbeiten hervorzuheben:

Die Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder hat sich in einem umfangreichen Bericht[5] u. a. mit der Thematik des digitalen Nachlasses befasst. Gegenstand der vorgenommenen Untersuchungen ist vor allem das postmortale Schicksal von Rechtspositionen, die der Erblasser aufgrund digitaler Kommunikation innehatte. Der Bericht geht insbesondere den Fragen nach, ob die Rechtsqualität von digitalen Daten gesetzlich zu bestimmen ist und ob gesetzgeberischer Handlungsbedarf besteht. Zu vielen Aspekten konnten sich bisher weder eine richtungsweisende Rechtsprechung noch eine gefestigte Literaturmeinung bilden. Das Bürgerliche Recht, das Urheberrecht, das Datenschutzrecht sowie das Telekommunikations- und Telemedienrecht wurden auf ihre Bedeutung für zivilrechtliche Fragestellungen untersucht.

Der Bericht sieht in den Anwendungsfällen des digitalen Nachlasses grundsätzlich keinen gesetzgeberischen Handlungsbedarf, räumt aber ein, dass sich beispielsweise in Bezug auf die Vererbbarkeit von Accounts die großen Anbieter nicht rechtskonform verhalten. Zwar schließen die meisten Anbieter in ihren AGB die Vererblichkeit nicht aus, sehen aber auch keine Übernahme des Vertrages durch die Erben vor. Obwohl Nutzungsrechte vererblich sind, sehen die AGB meist keine Regelungen vor, was mit den erworbenen digitalen Inhalten im Todesfall geschieht. Nach dem Grundsatz der Gesamtrechtsnachfolge geht der digitale Nachlass (einschließlich Accounts, Verträge, Auskunftsansprüche) gemäß § 1922 BGB auf die Erben über. Diesem Recht wird jedoch in den meisten AGB der Anbieter gar nicht hinreichend Rechnung getragen. Viele Kündigung- und Legitimationsklauseln sowie Klauseln zur Abwicklung des Vertrages nach dem Tod des Kunden sind unwirksam. Konkrete Empfehlungen für die Zielgruppen der vorliegenden Studie, die diesem Umstand abhelfen könnten, finden sich in dem Bericht der Arbeitsgruppe jedoch nicht.

[4] Eine Ausnahme könnte u. a. dann vorliegen, wenn eine Person über eine große Anzahl an „Followern“ verfügt und mit Posts in Social-Media-Kanälen Geld verdient. In diesem Fall kann es sich auch bei den hier genannten Werten um finanzielle Werte des digitalen Nachlasses handeln.

[5] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf.

Die Stellungnahme des Deutschen Anwaltvereins zum digitalen Nachlass[6] geht ebenfalls davon aus, dass der gesamte digitale Nachlass einschließlich Accounts, Verträgen und Auskunftsansprüchen gemäß § 1922 BGB auf die Erben übergeht und die zum großen Teil anders lautenden AGB der Anbieter einer Inhaltskontrolle nicht standhalten. Die Stellungnahme beschränkt sich jedoch auf Vorschläge zu ergänzenden Regelungen im TKG zur Auflösung der Diskrepanz zwischen Fernmeldegeheimnis und Erbrecht. Sie zeigt keine Handlungsoptionen dahingehend auf, was Erben, Erblasser, kleine und mittelständischen Unternehmen etc. schon heute tun können, um das faktische Ungleichgewicht zwischen Anbietern und Verbrauchern zu vermindern.

Verbraucherportale empfehlen den Verbrauchern zur frühzeitigen Regelung ihres digitalen Nachlasses,[7] mittels einer Vollmacht „über den Tod hinaus“ eine vertrauenswürdige Person zu bestimmen, damit diese sich im Todesfall um den digitalen Nachlass kümmert. Diese bevollmächtigte Vertrauensperson soll dazu Zugriff auf eine Liste bestehender Konten, Benutzernamen und Passwörter bekommen, um damit im Todesfall noch vor Ermittlung der Erben und von den Erben unabhängig tätig werden zu können – obwohl die Gefahr eines Widerrufs durch die Erben besteht. Zudem ist in vielen Fällen unklar, ob die Nutzung der Accounts durch die Vertrauensperson ohne Mitwirkung des Anbieters überhaupt rechtmäßig ist, und was mit den Accounts geschehen wird, wenn der Anbieter Kenntnis vom Todesfall des rechtmäßigen Nutzers bekommt. Auch der pragmatische Ansatz, bei dem der rechtmäßige Erbe Kenntnis von Accounts, Benutzernamen und Passwörter bekommt und diese einfach benutzt, ohne den Anbieter zu informieren, bedarf einer kritischen rechtlichen Analyse.

1.4 Aufbau der Studie

Im Anschluss an dieses Kapitel untersucht das Kapitel 2 auf Seite 35 den digitalen Nachlass aus Sicht des Erbrechts. Thematisiert werden u. a. die Vererbbarkeit digitaler Inhalte und die Befugnisse der Erben am digitalen Nachlass. Das Kapitel 3 auf Seite 53 fokussiert sodann digitale Angelegenheiten im Rahmen der Betreuung und Vorsorgevollmacht, insbesondere in Bezug auf den Umfang der Befugnisse des Betreuers und Vorsorgebevollmächtigten. Sodann diskutiert das Kapitel 4 auf Seite 83 datenschutzrechtliche Fragen, die im Zusammenhang mit dem digitalen Nachlass stehen, also u. a. die Frage nach einem absoluten Recht an personenbezogenen Daten und die Frage nach dem Umfang eines postmortalen Datenschutzes. Im Kapitel 5 auf Seite 115 werden sodann potenzielle Benachteiligungen der Verbraucher untersucht, die insbesondere in Zusammenhang mit den Allgemeinen Geschäftsbedingungen sowie dem Vergleich zu dem konkreten Dienstangebot stehen. In diesem Zusammenhang werden auch wichtige urheberrechtliche Aspekte des digitalen Nachlasses untersucht, die die Grundlage einer Bewertung von Benachteiligungen der Verbraucher bilden. In den darauf folgenden beiden Kapiteln stehen Vorsorgemöglichkeiten des Nutzers, siehe Kapitel 6 auf Seite 175, sowie vertragliche Vorsorgemöglichkeiten, siehe Kapitel 7 auf Seite 291, im Fokus der Untersuchung. In diesen Kapiteln wird jeweils zunächst der erbrechtliche Rahmen vorgestellt, um

[6] Stellungnahme Nr.: 34/2013, https://www.anwaltverein.de/de/newsroom/id-2013-34?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2013/SN-DAV34-13.pdf.

[7] Siehe z. B. das Verbraucherportal Baden-Württemberg: https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Digitaler+Nachlass+-+fruehzeitig+regeln.

im Anschluss daran u. a. technische Möglichkeiten aufzuzeigen, die den Erblasser und die Erben in der Vorsorge und praktischen Umsetzung und Durchsetzung eines digitalen Nachlasses unterstützen können. Die Studie fasst in Kapitel 8 auf Seite 337 Empfehlungen an die o. g. Zielgruppen – also Erben und Erblasser, Betreuer und Vorsorgebevollmächtigte, Unternehmen, Gesetzgeber und Verwaltung – zusammen und gibt in Kapitel 9 auf Seite 345 Mustervorlagen zur Vorbereitung eines digitalen Nachlasses.

1.5 Zusammenfassung

Die Rechte und Pflichten einer Person, die im Zusammenhang mit der Nutzung von IT-Systemen stehen, bilden den sogenannten „digitalen Nachlass." Dieser setzt sich u. a. aus finanziellen Werten, wie z. B. PayPal-Guthaben und gekauften E-Books, als auch aus ideellen Werten, wie z. B. einem Facebook-Profil und einem Online-Tagebuch, zusammen.

Aus heutiger Sicht befasst sich kaum ein Mensch mit dem Thema des digitalen Nachlasses. Dies liegt insbesondere daran, dass vielen Menschen nicht bewusst ist, dass und wie sie über ihren digitalen Nachlass verfügen können.

Ziel der vorliegenden Studie ist es daher, das Thema des digitalen Nachlasses in Bezug auf erbrechtliche, datenschutzrechtliche, verbraucherschutzrechtliche und technische Fragestellungen aufzuarbeiten und Empfehlungen für den Umgang mit dem digitalen Nachlass zu geben.

Das Wichtigste in Kürze

- Der digitale Nachlass setzt sich aus allen Rechten und Pflichten einer Person zusammen, die im Zusammenhang mit der Nutzung von IT-Systemen stehen.
- Finanzielle Werte des digitalen Nachlasses sind z. B. gekaufte E-Books.
- Ideelle Werte des digitalen Nachlasses sind z. B. Social-Media-Profile.
- Die Studie stellt die aktuelle rechtliche Situation zum Thema des digitalen Nachlasses dar.
- Die Studie zeigt auf und gibt Empfehlungen, mit welchen (technischen) Maßnahmen und (rechtlichen) Vorkehrungen der digitale Nachlass geregelt und praktisch umgesetzt bzw. für die Erben erleichtert werden kann.

2 Vererbbarkeit des digitalen Nachlasses

Dieses Kapitel untersucht

- die gesetzliche Ausgangslage hinsichtlich des digitalen Nachlasses;
- den Begriff und den Umfang des digitalen Nachlasses;
- die Befugnisse der Erben am digitalen Nachlass, insbesondere,
  - ob die Erben ein umfassendes Einsichtsrecht in Daten des Verstorbenen haben und
  - welche Rechte und Pflichten den Erben hinsichtlich der Online-Vertragsbeziehungen des Verstorbenen zukommen.

2.1 Relevanz des digitalen Nachlasses

Der Begriff des digitalen Nachlasses wurde in den letzten Jahren vielfach gebraucht und hat insbesondere durch die damit zusammenhängende Entscheidung des BGH noch einmal an Bedeutung gewonnen. Daher ist zunächst dieser Begriff zu definieren und die Vererbbarkeit des digitalen Nachlasses zu klären. Dabei muss auch eine Auseinandersetzung mit der Frage erfolgen, welche Befugnisse den Erben diesbezüglich zukommen. Die Klärung der gesetzlichen Ausgangslage ist zudem von Bedeutung für die Erarbeitung der Vorsorgemöglichkeiten des Nutzers. Nur was nach dem Gesetz zum Nachlass gehört, kann auch durch die privatautonome Vorsorge mittels letztwilliger Verfügungen auf die Erben übertragen werden.

2.2 Allgemeines: Vererbbarkeit digitaler Inhalte nach geltender Rechtslage

Der mittlerweile gängig verwendete Begriff „digitaler Nachlass“ beschreibt keine erbrechtliche Sonderkategorie, sondern ist lediglich Sammelbegriff für die gesamte digitale Hinterlassenschaft des Verstorbenen.[1] Der Übergang von Todes wegen richtet sich im Grundsatz nach den allgemeinen Regeln der Universalsukzession gemäß § 1922 I BGB.[2] Der Begriff wird verschiedentlich definiert, beispielsweise als „Gesamtheit des digitalen Vermögens des Erblassers“[3] oder „Gesamtheit der Rechtsverhältnisse des Erblassers betreffend informationstechnische Systeme einschließlich des gesamten elektronischen Datenbestands des Erblassers.“[4] Dazu werden unter anderem auf lokalen Speichermedien gesicherte Daten, Daten im Internet oder in Clouds, vertragliche Beziehungen des Erblassers zu Dienstanbietern beruflicher und sozialer Netzwerke[5] oder Online-Bezahldiensten, Onlinebanking, Nutzungsrechte an Musik- oder Sprachwerken,[6] Streamingportalen sowie Online-Spielen[7] und auch Kryptowährungen[8] gezählt.

Hinsichtlich des Übergangs im Rahmen der Universalsukzession ist dabei zunächst danach zu unterscheiden, ob der digitale Nachlass sich auf einem lokalen Datenträger bzw. einem eigenen Server des Erblassers befindet oder auf einem fremden Server gespeichert ist.

Lokale Datenträger oder Speichermedien sind eine Sache im Sinne von § 90 BGB, an der Eigentum des Erblassers besteht. Dieses Eigentum geht nach § 1922 I BGB im Wege der Universalsukzession

[1] *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK, BGB § 1922 Rn. 381.
[2] *BGH*, NJW 2018, 3178.
[3] *Herzog*, NJW 2013, S. 3745.
[4] *Deusch*, ZEV 2014, S. 2 (2 f.).
[5] Mit grundsätzlichen Fragen zur Vererbbarkeit eines Accounts bei einem sozialen Netzwerk hat sich der BGH im Juli 2018 befasst, vgl. BGH, NJW 2018, 3178.
[6] *Lydiga*, ZEV 2018, S. 1 (2).
[7] *Kunz*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1922 Rn. 594.
[8] *Amend-Traut/Hergenröder*, ZEV 2019, S. 113 (116 f.).

auf die Erben über. Die auf dem Datenträger gespeicherten Daten teilen das Schicksal des Speichermediums und stehen nach dem Tod des Erblassers ebenfalls den Erben zu.[9]

Auch Daten, die auf einem fremden Server gespeichert sind, gehen grundsätzlich nach den erbrechtlichen Grundsätzen auf die Erben über.

Online-Vertragsbeziehungen

Dabei kann es sich einerseits um Nutzungsverträge über soziale oder berufliche Netzwerke bzw. über E-Mail-Konten (user-account-Verhältnisse[10]) handeln. Diesen liegt ein schuldrechtlicher Vertrag zwischen Erblasser und dem Dienstanbieter zugrunde, der nach § 1922 I BGB mit seinen sämtlichen Rechten und Pflichten auf die Erben übergehen kann, indem die Erben grundsätzlich zunächst in den Vertrag eintreten.[11]

Auch weitere Rechtsbeziehungen gehören zum Nachlass, so sämtliche Online-Vertragsbeziehungen mit Vermögenswert wie Avatare sowie Guthaben bei Online-Spielen, Guthaben auf Bonuskarten, bei Online-Bezahldiensten oder Onlinebanking; aber auch in einer Cloud gespeicherte Daten,[12] Online-Tagebücher und Apps ohne Vermögenswert,[13] die auf einem fremden Server gespeichert sind.[14]

Nutzungsrechte des Erblassers an digitalen Inhalten wie Streamingdiensten, Domains, Lizenzverträgen oder Nutzungsrechte an Programmen sind ebenfalls grundsätzlich vererblich, wobei hier gegebenenfalls urheberrechtliche Beschränkungen zu beachten sind.[15]

Das Gleiche gilt für Vertragsbeziehungen, im Rahmen derer der Erblasser persönlichkeitsrelevante Inhalte schafft oder teilt. Etwas anderes folgt auch nicht aus dem Rechtsgedanken der § 399 oder § 39 BGB. Danach kann sich aus dem Wesen eines Vertrages seine Unvererbbarkeit ergeben, wenn die diesbezüglichen Leistungspflichten der Vertragsparteien derart auf die Person des Berechtigten oder Verpflichteten zugeschnitten sind, dass ein Subjektswechsel die Leistung in ihrem Wesen verändern würde, die Leistungspflichten also höchstpersönlicher Natur sind. Der Dienstanbieter eines digitalen Dienstes erbringt jedoch gegenüber jedem Nutzer dieselben (rein technischen) Leistungen, namentlich die zur Verfügungstellung der Kommunikationsplattform, Veröffentlichung und Zugänglichmachung von Inhalten und Übermittlung von Nachrichten gemäß Beauftragung durch den Nutzer. Diese Leistungspflicht ist nicht individuell auf den Nutzer bezogen, sondern besteht gegenüber jedem Nutzer gleichermaßen, ist also nicht höchstpersönlich.[16] Zudem kann sie unverändert auch gegenüber den Erben als neuen Vertragspartnern erbracht werden.

[9] *Hoeren*, NJW 2005, S. 2113 (2114).
[10] *Kunz*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1922 Rn. 603.
[11] BGH, NJW 2018, 3178 (3179).
[12] Hinsichtlich der Vererbbarkeit eines solchen Vertrages nun auch ausdrücklich LG Münster, Urteil vom 16.04.2019 – 14 O 565/18.
[13] *Kunz*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1922 Rn. 595.
[14] *Kunz*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1922 Rn. 601.
[15] *Preuß*, in: Gsell u. a. (Hrsg.) BeckOGK BGB, § 1922 Rn. 397; siehe hierzu ausführlich Kapitel 5 auf Seite 115.
[16] BGH, NJW 2018, 3178 (3180 f.); *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 339; mit demselben Ergebnis aber mittels Parallelwertung zur Vereinsmitgliedschaft: *Willems*, ZfPW 2016, S. 494 (506).

Dies gilt nicht nur für die von der höchstrichterlichen Rechtsprechung bisher behandelten Social-Media-Accounts, sondern lässt sich auch (ohne Anspruch auf Vollständigkeit) auf E-Mail-Accounts, Online-Spiele, vom Erblasser geschaffene Websites, Blogs und Online-Tagebücher übertragen.

Eine Ausnahme hiervon gilt lediglich für Online-Partnerschaftsvermittlungsverträge, die ausnahmsweise aufgrund ihres individuellen Zuschnitts der Leistungspflichten als höchstpersönlich einzustufen sind. Ziel eines solchen Vertrages ist es, dass der Anbieter für den Nutzer eine Partnerschaft anbahnen soll. Diese Partnervermittlung ist jedoch auf den jeweiligen Nutzer höchstpersönlich zugeschnitten.[17] Insoweit ergeben sich keine Besonderheiten zur Rechtsprechung analog geschlossener Partnerschaftsvermittlungsverträge.[18]

Nutzungsrechte

Zu untersuchen ist auch, wie die Vererbbarkeit von rein digital gespeicherten Inhalten wie E-Books, Musik oder Filmen zu behandeln ist. Dazu muss zunächst geklärt werden, welche Rechtsposition dem Erblasser als Nutzer an diesen Inhalten zukommt. Einerseits könnte anzunehmen sein, dass der Nutzer durch den Download Eigentum an der Datei erhält. Andererseits könnte durch die Anbieter auch lediglich ein Nutzungsrecht eingeräumt sein. Weiterhin wäre möglich, dass wiederum die Verfügungsbefugnis an den Daten dem Speichermedium folgt. Hinsichtlich E-Books könnte beispielsweise dann anzunehmen sein, dass der Erbe durch den Erwerb des Eigentums am sogenannten „E-Reader“ auch das Eigentum an den darauf gespeicherten Büchern erlangt.
Diesbezüglich ist jedoch die Besonderheit zu beachten, dass die E-Books nicht ausschließlich mit dem E-Reader als Speichermedium verknüpft sind, sondern mit einem Nutzerkonto (z. B. einem Amazon-Account), und der Erblasser auch über andere Medien auf „seine“ E-Books zugreifen kann, beispielsweise mittels einer App auf seinem Handy oder Laptop.
Insofern handelt es sich jedenfalls nicht um ein mithilfe des E-Readers verkörpertes Werk, das mit einem gegenständlichen analogen Buch gleichgesetzt werden kann, welches eine Person in Händen hält, sondern rein tatsächlich kann von mehreren Kanälen auf die Bücher zugegriffen werden. Das Werk befindet sich auch nach Erwerb noch auf einem Server des Dienstanbieters. Dem Erwerber wird diesbezüglich lediglich ein Nutzungsrecht eingeräumt, was sich insbesondere aus den AGB der Anbieter ergibt.[19]

Gleiches gilt für digital gespeicherte Musikbibliotheken und .mp3-Dateien. Aus rein erbrechtlicher Sicht ist jedoch auch hier das aus der Vertragsbeziehung zwischen Erblasser und Dienstanbieter folgende Nutzungsrecht grundsätzlich nach § 1922 I BGB vererblich.

Kryptowährungen

Auch die erbrechtliche Behandlung von Kryptowährungen wurde untersucht.[20] Auf eine durch den Bundestag vorgelegte Anfrage antwortete die Bundesregierung, dass der Grundsatz der Universal-

[17] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 340.
[18] *AG Dortmund*, NJW-RR 1991, 689.
[19] Vgl. zu den AGB ausführlich Kapitel 5 auf Seite 115.
[20] Allgemein zur Funktionsweise vgl. bspw.: *Schlund/Pongratz*, DStR 2018, S. 598.

sukzession „auch für Guthaben in Kryptowährungen, die der Erblasser erworben hatte“[21] gilt. Das für den erbrechtlichen Vermögensübergang maßgebliche Bezugsobjekt ist jedoch schwer zu bestimmen. Jedenfalls sind weder die kryptografischen Währungseinheiten an sich eigentumsfähige Sachen im Sinne von §§ 90, 903 ff. BGB,[22] noch sind die zugrunde liegenden Daten auf einem lokalen Datenträger des Erblassers gespeichert.[23] Auch die Vererbbarkeit einer Forderung scheidet aus, da es einerseits keine Instanz gibt, die die Kryptowährungen ausgibt oder kontrolliert. Diese werden stattdessen von den Nutzern eines offen ausgestalteten und für jeden zugänglichen Peer-to-Peer-Computernetzwerks gemeinsam erschaffen und verwaltet.[24] Daher steht kein Rechtssubjekt zur Verfügung, gegen das die Forderung gerichtet werden könnte. Zudem steht dem einzelnen Nutzer an diesen im Netzwerk abgespeicherten Daten keine insoweit rechtlich relevante Rechtsinhaberschaft oder ein damit korrespondierender Anspruch zu. Vertreten wird daher, dass vielmehr der kryptografische Schlüssel (Private Key) vererbbar ist, da durch diesen dem Nutzer die „*faktische Verfügungsgewalt* über die seiner öffentlichen Adresse zugeordneten virtuellen Vermögenswerte ermöglicht“ wird. Verliert ein Nutzer den Private Key, verliert er auch die Verfügungs- und Zugriffsmöglichkeit über sein in kryptografischen Währungen bestehendes Guthaben. Zugegeben wird zwar, dass auch diese „aus der Inhaberschaft am privaten Schlüssel resultierende faktische Verfügungsgewalt für sich betrachtet keine Rechtsposition dar[stellt].“[25] Jedoch könne der Private Key auf einem lokalen Speichermedium des Erblassers oder in Papierform gesichert werden, durch welches dann Eigentum vermittelt werden könne. Daneben könnte der Erblasser den Private Key auch in einem „Online-Wallet“ gespeichert haben und der Erbe die Verfügungsbefugnis darüber sowie den Private Key durch Eintritt in die Vertragsbeziehung zwischen Erblasser und Anbieter erlangen.[26]

2.3 Befugnisse des/der Erben am digitalen Nachlass

Nicht abschließend geklärt ist bisher jedoch, welche Befugnisse dem oder den Erben an den digitalen Werten zukommen. Hier ist zunächst danach zu differenzieren, welche Rechtsnatur dem im Einzelfall infrage stehenden digitalen Nachlassbestandteil zukommt. Weiterhin stellt sich die Frage, ob aus der grundsätzlichen Vererbbarkeit von Daten bzw. der Vertragsverhältnisse mit Dienstanbietern auch ein unbeschränktes Recht der Erben auf Zugriff sowie Einsicht folgt. Insbesondere hinsichtlich der Rechtsbeziehungen zu Dienstanbietern stellt sich die darüber hinausgehende Frage, ob den Erben auch ein Recht auf Weiterführung der Vertragsbeziehung bzw. Weiternutzung der Daten zusteht.[27]

[21] Bt-Drucks. 19/3068, S. 29.
[22] *Schlund/Pongratz*, DStR 2018, S. 598.
[23] *Amend-Traut/Hergenröder*, ZEV 2019, S. 113 (117).
[24] *Amend-Traut/Hergenröder*, ZEV 2019, S. 113 (114 f.).
[25] Insgesamt hierzu und zum vorhergehenden *Amend-Traut/Hergenröder*, ZEV 2019, S. 113 (117).
[26] *Amend-Traut/Hergenröder*, ZEV 2019, S. 113 (117 f.).
[27] Zu dieser gängigen Differenzierung vgl. bspw. *Raude*, RNotZ 2017, S. 17 (20); *Preuß*, NJW 2018, S. 3146 (3148); *Herzog*, NJW 2013, S. 3745 (3749 f.); *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 339.

2.3.1 Einsichtsrecht

Zu klären ist zunächst, ob die Erben berechtigt sind, die zum digitalen Nachlass gehörenden Daten einzusehen bzw. in Accounts des Erblassers Einsicht zu nehmen.

2.3.1.1 Einsichtsrecht unter erbrechtlicher Betrachtung

Hinsichtlich des Einsichtsrechts könnte sich aus erbrechtlicher Sicht dabei insbesondere die Höchstpersönlichkeit der Daten als problematisch darstellen.

Jedenfalls hinsichtlich der auf einem lokalen Datenträger gespeicherten Daten gilt jedoch grundsätzlich, dass diese das Schicksal des Speichermediums teilen und mit dem Eigentum an diesem auf die Erben übergehen.[28] Insoweit ist der allgemeine Grundsatz anzuwenden, dass der Erbe als Eigentümer des Mediums, auf dem die Information verkörpert ist, auch die Verfügungsbefugnis über die Information erhält, unabhängig davon, ob sich diese analog auf Papier oder auf einem Datenträger befindet.[29]

Auch die als neue Vertragspartner in den Vertrag eintretenden Erben haben einen Anspruch auf Zugang zu den Benutzerkonten des Erblassers und Einsicht in die darin enthaltenen (digitalen) Inhalte.[30] Sie sind nun Berechtigte hinsichtlich der Daten, die weiterhin auf den Servern der Dienstanbieter gespeichert sind.

Nach nun höchstrichterlich bestätigter und auch hier vertretener Ansicht ist hinsichtlich der Vererbbarkeit nicht danach zu unterscheiden, ob die Daten vermögensrechtlichen oder höchstpersönlichen Inhalt haben, was sich bereits aus der gesetzlichen Wertung der § 2047 II und § 2373 S. 2 BGB ergibt.[31] Diese Normen setzen – auch wenn sie dies nicht ausdrücklich regeln – den Übergang von (verkörperten) Rechtspositionen mit höchstpersönlichem Inhalt ohne Rücksicht auf ihren Vermögenswert auf die Erben voraus. Unstreitig gehören nach diesen Normen auch höchstpersönliche analoge Dokumente, wie Tagebücher oder Briefe, aber auch Fotos, zur Erbmasse. Das Gesetz kennt diesbezüglich also keine Differenzierung von höchstpersönlichem oder vermögensrechtlichem Nachlass. Eine solche Differenzierung nach dem Umfang des Erbrechts sollte auch nicht vom Speichermedium abhängig gemacht werden. Die Probleme der Höchstpersönlichkeit stellen sich aus erbrechtlicher Sicht unabhängig von der Verkörperung, also insbesondere davon, ob der Inhalt digital gespeichert oder analog verfasst wurde. Nicht nur würde eine derartige Unterscheidung dem Grundsatz der Universalsukzession widersprechen, auch würde dies zu erheblichen praktischen Problemen im Rahmen der damit notwendigen Durchsicht und Zuordnung sämtlicher digitaler Inhalte führen.[32]

[28] *Hoeren*, NJW 2005, S. 2113 (2114).
[29] *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1922 Rn. 391.
[30] BGH, NJW 2018, 3178 (3179).
[31] Zu dieser Ansicht insbesondere *Hoeren*, NJW 2005, S. 2113 (2114); a.A. statt aller *Herzog*, NJW 2013, S. 3745 (3749); eindeutig auch *BGH*, NJW 2018, 3178 (3182).
[32] Insgesamt hierzu BGH, NJW 2018, 3178 (3182 f.).

Somit ist der Zugang der Erben zu den Nutzerkonten des Erblassers jedenfalls aus erbrechtlichen Gründen nicht zu beschränken.

2.3.1.2 Einsichtsrecht unter datenschutzrechtlicher Betrachtung

Datenschutzrechtliche Belange des Erblassers sind von einem Zugangsrecht der Erben auf dessen Nutzerkonten nicht betroffen, da die DSGVO gemäß Erwägungsgrund 27 DSGVO nicht auf personenbezogene Daten Verstorbener anzuwenden ist. Der BGH hat die Frage der Anwendung der DSGVO im Hinblick auf die der Zugangsgewährung für die Erben immanente Verarbeitung von inhaltlichen Daten etwaiger Kommunikationspartner offen gelassen, da jedenfalls eine solche Verarbeitung (in dem zu entscheidenden Fall durch den Betreiber eines sozialen Netzwerks) nach Art. 6 I 1 lit. b und lit. f DSGVO gerechtfertigt sei.[33]

Zu beachten ist, dass es im konkreten Fall um die Frage der datenschutzrechtlichen Konformität der Datenverarbeitung durch den Betreiber des sozialen Netzwerks ging. Hiervon zu unterscheiden ist die Frage der datenschutzrechtlichen Konformität einer Datenverarbeitung durch die Erben. Diese Frage kann beispielsweise in solchen Konstellationen relevant sein, wenn bereits der Erblasser datenschutzrechtlich Verantwortlicher war, wie z. B. bei Speicherung personenbezogenen Daten seiner Vertragspartner (Kunden) mittels Cloud Computing. War die Nutzung der Online-Dienste bereits für den Erblasser nicht mit datenschutzrechtlichen Pflichten verbunden, beispielsweise aus dem Grund, weil die Bereichsausnahme nach Art. 2 II lit. c DSGVO einschlägig war, so stellen sich für die Erben ebenfalls keine datenschutzrechtlichen Pflichten, sofern sie den Zugang zum betreffenden Online-Dienst ebenfalls zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten nutzen.

Ist der Erblasser bereits datenschutzrechtlich Verantwortlicher gewesen, der die Datenverarbeitung nach Art. 6 I 1 lit. b DSGVO gerechtfertigt hat, kann der Zugang auf den Account des Erblassers durch die Erben zu den bisherig verfolgten Zwecken ebenfalls nach dieser Vorschrift gerechtfertigt sein. Hierbei ist zunächst festzuhalten, dass die Gesamtrechtsnachfolge lediglich einen juristischen Vorgang darstellt, sodass sie auch keine Übermittlung oder eine andere Form der Datenverarbeitung darstellt.[34] Da eine Universalsukzession das Vertragsverhältnis nicht verändert, kann eine Datenverarbeitung durch Gesamtrechtsnachfolge auf Art. 6 I 1 lit. b DSGVO gestützt werden.[35]

Darüber hinaus kommt auch der Rechtfertigungsgrund des Art. 6 I 1 lit. f DSGVO in Betracht. Danach liegt eine rechtmäßige Datenverarbeitung vor, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. In dem oben genannten Fall, in welchem es um die datenschutzrechtliche Rechtmäßigkeit der Verarbeitung durch den Dienstanbieter ging, gelangte der BGH u.a. auch durch eine Abwägung nach Art. 6 I 1 lit. f DSGVO zu der Rechtmäßigkeit der Datenverarbeitung. Hierbei stellte der BGH

[33] BGH NJW 2018, 3178 (3185).
[34] *Schantz*, in: *Simitis/Hornung/Spiecker*, DSGVO Art. 6 Rn. 23.
[35] *Schantz*, in: *Simitis/Hornung/Spiecker*, DSGVO Art. 6 Rn. 23.

fest, dass die Verarbeitung zur Wahrung berechtigter Interessen der Erben erforderlich ist, und die Interessen und Grundrechte der Kommunikationspartner nicht überwiegen.

Obwohl die Frage der Zulässigkeit einer Datenverarbeitung aufgrund von berechtigten Interessen grundsätzlich von den konkreten Umständen des betroffenen Einzelfalls abhängig und dementsprechend auch einzelfallbezogen zu ermitteln und zu beurteilen ist,[36] können einige in dem Urteil getroffenen Ausführungen generell auf das infrage stehende Zugangsrecht durch die Erben übertragen werden: Zum einen stellt das in Art. 14 I 1 GG geschützte Erbrecht und die daraus folgende Geltendmachung vertraglicher Ansprüche der Erben als Rechtsnachfolger gegenüber dem Dienstanbieter ein berechtigtes Interesse dar. Zum anderen kann ein über das allgemeine berechtigte Interesse der Erben hinaus auch ein vermögensrechtliches Interesse bestehen. Im konkreten Fall führte der BGH die Abwehr etwaiger haftungsrechtlicher Ansprüche von Dritten als berechtigtes Interesse an, wobei der BGH klarmachte, dass die Geltendmachung, Ausübung und Verteidigung eigener Rechte ein berechtigtes Interesse für die Datenverarbeitung darstellt.[37] Insbesondere bei einem Zugang durch die Erben zur Nachlassabwicklung dürfte dieser Punkt relevant sein.

Aufseiten der Kommunikationspartner des Erblassers sind das Grundrecht aus Art. 8 I GRCh auf Schutz ihrer personenbezogenen Daten und das Grundrecht auf Achtung des Privat- und Familienlebens und der Kommunikation nach Art. 7 GRCh zu berücksichtigen. Erwägungsgrund 47 S. 1 DSGVO nennt als Gesichtspunkt der Interessenabwägung „die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“. Es ist nach Erwägungsgrund 47 S. 3 DSGVO auch zu berücksichtigen, ob die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Bei der Nutzung von Online-Diensten übermitteln die Nutzer die sie betreffenden personenbezogenen Daten (etwa in Form von Nachrichten, E-Mails, geteilte Bilder, etc.) freiwillig und bewusst an den Dienstanbieter bzw. Empfänger, sodass sie die Verfügungsbefugnis hierüber insoweit aufgeben.[38] Sie können auch vernünftigerweise absehen, dass die Datenverarbeitung auch nach dem Tod des Erblassers fortgesetzt wird und insoweit Erben Kenntnis über diese Daten erlangen könnten.

Hiervon ausgehend dürfte ein Zugang auf den Account des Erblassers durch die Erben insoweit keine datenschutzrechtlichen Probleme bereiten, als die Erben keine weitergehenden Zwecke mit der Datenverarbeitung verfolgen (z. B. die Daten der Kommunikationspartner einem unbestimmten, nicht mehr zu kontrollierenden Personenkreis zu offenbaren). Es ist daher zu beachten, dass der Zugang auf die zur Nachlassabwicklung erforderliche Datenverarbeitung (wie z. B. Identifikation möglicher Gläubiger und Schuldner des Erblassers und deren Kommunikationsdaten, Sichtung von vertraglichen Absprachen, etc.) beschränkt bleibt.

[36] BGH, NJW 2018, 3178 (3185 ff.).
[37] BGH, NJW 2018, 3178 (3186 ff.).
[38] Vgl. BGH, NJW 2018, 3178 (3187).

2.3.2 Aktive Nutzung

Insbesondere hinsichtlich der Vertragsbeziehungen des Erblassers mit Online-Dienstanbietern stellt sich die Frage, ob die Erben befugt sind, diese als Rechtsnachfolger des Erblassers weiterzuführen. Zwar ist unstreitig, dass die Erben durch den Erbfall zunächst in die Vertragsbeziehungen des Erblassers eintreten. Fraglich ist jedoch insbesondere, auch wenn sich diese Frage im Grundsatz bei allen Online-Vertragsbeziehungen des Erblassers stellt, wie es rechtlich zu behandeln ist, wenn die Erben beispielsweise eine personalisierte Website oder einen Social-Media- bzw. E-Mail-Account des Erblassers im Einzelfall weiterführen wollen.

Dabei kommt es nicht allein darauf an, ob der Vertrag aus Sicht des Erblassers zu rein geschäftlichen (wie bei beruflich genutzten Benutzerprofilen) oder vermögensrechtlichen (wie bei Guthaben bei Online-Bezahldiensten oder bei Onlinebanking) Zwecken geschlossen wurde oder ob der Erblasser auf – ihm aufgrund des Vertrages mit dem Dienstanbieter zur Verfügung gestellten – Accounts oder Websites persönlichkeitsrelevante Inhalte geschaffen oder kommuniziert hat. Der Personenbezug der geteilten Inhalte ist im Grundsatz unabhängig von der Vertragsgestaltung und den verabredeten Leistungspflichten zwischen Erblasser und Dienstanbieter. Nach herrschender Ansicht sind diese Verträge aber insoweit personenbezogen, als nur der Nutzer selbst berechtigt ist, über sein Konto Nachrichten zu versenden und Inhalte zu veröffentlichen.

In der höchstrichterlichen Rechtsprechung wurde die Frage der erbrechtlichen Behandlung eines aktiven Weiternutzungsrechts der Erben bisher offengelassen, da diese Frage nicht streitgegenständlich war. Lediglich angedeutet wurde, dass ein etwaiger Personenbezug nicht die Unvererbbarkeit der Leistungspflicht des Dienstanbieters (Zurverfügungstellung der Plattform) zur Folge habe und der Dienstanbieter nicht schutzwürdig dahingehend sei, diese nicht gegenüber den Erben erbringen zu müssen. Allerdings „könnte [dies] dazu führen, dass – wie beim Girovertrag – die aktive Weiternutzung des Kontos des Erblassers durch den Erben, die in der Praxis ohnehin regelmäßig nicht beabsichtigt sein wird, nicht von seinem Erbrecht umfasst ist.“[39]

2.3.2.1 Aktive Nutzung aus erbrechtlicher Sicht

Auch in der Literatur ist diese Frage – immer noch – umstritten.

Keinerlei Weiternutzungsrecht des Erben

Nach einer Ansicht handelt es sich zumindest bei der Nutzung des Profils bei einem sozialen Netzwerk um ein höchstpersönliches Recht des Erblassers, das mit seinem Tode untergeht. Da gerade die Bearbeitung und Nutzung des Profils eines Social-Media-Accounts aber höchstpersönliches Recht des Erblassers sei, hätten die Erben keinen Anspruch auf Veränderung des Accounts gegen den Dienstanbieter, weil „mit dem Tod eine freie Entfaltung der Persönlichkeit des Verstorbenen

[39] BGH, NJW 2018, 3178 (3181).

nicht mehr in Betracht kommt." Der Nutzungsvertrag zwischen Dienstanbieter und Erblasser sei aufgrund des Personenbezugs der Hauptleistungspflicht als überwiegend personenbezogen einzuordnen. Leistungspflicht des Dienstanbieters sei nicht nur die Bereitstellung der Plattform, für die er im Gegenzug die Mitgliedschaft des Nutzers erhalte. Vielmehr knüpfe die Mitgliedschaft unmittelbar an die Person des Nutzers an, eine Übertragung sei nicht möglich. Daraus wird der Schluss gezogen, dass „die Übernahme eines Facebook-Profils oder von dessen Zugang sowie die Bearbeitung oder Löschung durch Erben nicht möglich" sei. Insofern könne auch dem Schuldner der Wechsel des Vertragspartners unzumutbar sein und die Unvererblichkeit auf der Schutzwürdigkeit des Dienstanbieters beruhen.[40]

Begründung eines eigenen Rechtsverhältnisses durch Weiternutzung des Accounts

Auch die wohl herrschende Ansicht stuft das Recht auf aktive Nutzung des Accounts – soweit der Nutzungsvertrag an sich als höchstpersönlich und nicht rein geschäftlich einzustufen sei[41] – aufgrund seines Personenbezugs als höchstpersönliches Recht des Erblassers ein und geht daher von dessen Unvererbbarkeit aus. Die aktive Nutzungsmöglichkeit soll mit dem Tod des Erblassers erlöschen.[42]

Trotzdem gehe jedoch das Vertragsverhältnis und damit der Account an sich zunächst auf den Erben über. Dieser gehört zum Nachlass. Verwende der Erbe den Account dann jedoch selbst, entstehe ein eigenes neues Vertragsverhältnis zum Dienstanbieter. Die aktive Nutzung des Accounts durch die Erben sei daher nicht lediglich Fortführung des Altvertrages zwischen Erblasser und Dienstanbieter, sondern es entstehe ein eigener (neuer) Vertrag zwischen Erben und Dienstanbieter, wie dies auch im Rahmen der Vererbbarkeit von Giroverträgen[43] angenommen wird.[44] Dies gelte aber nur dann, wenn die Erben das Konto wie ein eigenes nutzen. Wird das Konto lediglich zur Abwicklung nachlassbezogener Geschäfte genutzt, soll der Nutzungsvertrag als ein vom Erblasser abgeleitetes Rechtsverhältnis fortgesetzt und kein eigenes Rechtsverhältnis begründet werden.[45]

Im Grundsatz sei eine Vertragsfortführung mit den Erben nicht unzumutbar für den Dienstanbieter, da der Vertrag zwischen Nutzer und Dienstanbieter in der Regel ohne Rücksicht auf die Person und auch ohne nähere Identitätsprüfung abgeschlossen wird.[46] Allerdings wurde in der Entscheidung des *BGH* angedeutet, dass die aktive Fortführung des Kontos durch die Erben für den Dienstanbieter und damit ein Wechsel des Kontoberechtigten deshalb unzumutbar sein könne, weil dadurch die Rechte des Dienstanbieters an den individuellen Daten des Erblassers beeinträchtigt würden.[47]

[40] Zum Ganzen: *Klas/Möhrke-Sobolewski*, NJW 2015, S. 3473 (3474).
[41] *Raude*, RNotZ 2017, S. 17 (20).
[42] So ausdrücklich *Preuß*, NJW 2018, S. 3146 (3148).
[43] Zum Schicksal des Girovertrages bei Vor- und Nacherbfolge BGH, NJW 1990, 190.
[44] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 338; *Raude*, RNotZ 2017, 17 (20); *Preuß*, NJW 2018, 3146 (3148); *Herzog*, NJW 2013, 3145 (3749 f.); *Gloser*, MittBayNot 2016, 12 (14); *Pruns*, NWB 2013, 3161 (3164 f.); *Kutscher*, Der digitale Nachlass, S. 101.
[45] *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1922 Rn. 396, 242.
[46] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 339; *Gloser*, MittBayNot 2016, S. 12 (14); *Kutscher*, Der digitale Nachlass, S. 102.
[47] BGH, NJW 2018, 3178 (3181).

Vertragseintritt des Erben in sämtliche Rechte und Pflichten

Nach anderer Ansicht tritt der Erbe in die Vertragsbeziehung ein und ist befugt, den Account selbst zu nutzen, Nachrichten zu versenden, „die Profilseite um eigene Informationen [zu] ergänzen“ und somit das Vertragsverhältnis selbst fortzuführen.[48] Zu unterscheiden sei zwischen der Kontoinhaberschaft und dem Einsichtsrecht in archivierte Inhalte.[49] Dabei werden weder die Kontoinhaberschaft[50] noch das Einsichtsrecht[51] als höchstpersönliche Rechte des Nutzers eingestuft, weshalb der Erbe gemäß § 1922 BGB in sämtliche Rechte und Pflichten des Vertrages eintrete. Die Rechtsposition des Nutzers erschöpfe sich in der vertraglichen Rahmenbeziehung. Daher sei ihm „die Weiterführung des gesamten E-Mail-Accounts unter Beibehaltung der bisherigen E-Mail-Adresse ermöglicht.“[52] Im Rahmen der Weiternutzung eines Social-Media-Accounts sei aber zum Schutz des postmortalen Persönlichkeitsrechts des Erblassers zumindest die Profilseite (Benutzername, Fotos und sonstige Informationen) an die Person des Rechtsnachfolgers anzupassen.[53]

Stellungnahme

Der Ansicht, die bei Weiternutzung des Accounts von einer Neubegründung des Vertrages zwischen Rechtsnachfolger und Dienstanbieter ausgeht, ist zuzustimmen. Im Ausgangspunkt ist es richtig, dass es sich bei der aktiven Nutzung eines Accounts (sei es eines E-Mail- oder Social-Media-Accounts) um ein höchstpersönliches Recht des Nutzers handelt. Dieses Recht ist immer auf die Person bezogen, die Accounts oder Websites im eigenen Interesse und aus eigenem Recht nutzen will. Daraus kann aber nicht der Schluss gezogen werden, dass insgesamt das Nutzungsrecht an dem Account mit dem Tod des Nutzers untergeht. Weder der Rechtsverkehr noch der Dienstanbieter haben ein schutzwürdiges Vertrauen daran, dass „tote Accounts“ entstehen. Hat der Erbe tatsächlich einmal ein Interesse daran, den Vertrag fortzuführen, ist ausreichender Schutz dadurch gewährt, dass ein neues Vertragsverhältnis entsteht. Insoweit kann es zumindest bei privaten Accounts erforderlich werden, Nachfolgehinweise zu geben, um eine Verletzung des postmortalen Persönlichkeitsrechts des Erblassers zu vermeiden. Unter Berücksichtigung dessen ist auch rechtlich kein Vorteil darin ersichtlich, wenn der Erbe als Rechtsnachfolger in den Altvertrag des Erblassers eintritt, vor allem, da auch in diesem Fall eine Anpassung des Nutzungsverhältnisses an den Erben erforderlich wird.

Zu beachten ist jedoch, dass die Begründung eines neuen Vertragsverhältnisses durch Weiternutzung der Erben nicht den zunächst nach dem Erbfall bestehenden Anspruch auf Zugangsgewährung und Einsicht einschränkt.[54]

[48] *Seidler*, Digitaler Nachlass, S. 140.
[49] *Seidler*, Digitaler Nachlass, S. 92.
[50] *Seidler*, Digitaler Nachlass, S. 88 ff. für E-Mail-Accounts, S. 134 ff. für Soziale Netzwerke.
[51] *Seidler*, Digitaler Nachlass, S. 95 ff. für E-Mail-Accounts, S. 136 f. für Soziale Netzwerke.
[52] *Seidler*, Digitaler Nachlass, S. 95.
[53] *Seidler*, Digitaler Nachlass, S. 136.
[54] So auch *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 340: Eines gesetzgeberischen Tätigwerdens bedürfe es insoweit nicht.

2.3.2.2 Aktive Weiternutzung aus datenschutzrechtlicher Sicht

Aus datenschutzrechtlicher Sicht stellen sich in Bezug auf Social-Media-, Onlinebanking- sowie E-Mail-Accounts im Wesentlichen dieselben Fragen, die bereits oben bei der Frage des Einsichtsrechts durch die Erben besprochen wurden; es kann insoweit auf die obigen Ausführungen verwiesen werden. Bei der Frage der Rechtmäßigkeit der Datenverarbeitung ist allerdings auf die konkrete Datenverarbeitung – die vielerlei Formen haben kann, wie z. B. das Markieren von Personen auf Fotos, Teilen mit weiteren Freunden, etc. – abzustellen und zu fragen, ob hierfür die bereits oben angesprochene Interessenabwägung nach Art. 6 I 1 lit. f DSGVO zugunsten der Erben den Ausschlag gibt. Eine pauschale Beantwortung der Frage, ob eine Weiternutzung datenschutzrechtlich zulässig ist, kann daher nicht getroffen werden, sondern es sind die konkreten Interessen an der jeweiligen Form der Datenverarbeitung gegeneinander abzuwägen.

Ob die Erben datenschutzrechtliche Pflichten treffen, hängt zunächst davon ab, ob deren konkrete Nutzung in den Anwendungsbereich der DSGVO fällt. Soll die aktive Weiternutzung ausschließlich für persönliche oder familiäre Tätigkeiten erfolgen, ist bereits der Anwendungsbereich der DSGVO nicht eröffnet, Art. 2 DSGVO. Es fallen dann keine datenschutzrechtlichen Pflichten für die Erben an.

War die Nutzung des Accounts bereits für den Erblasser mit datenschutzrechtlichen Pflichten verbunden, so wird dies regelmäßig auch für die Erben gelten, die anstelle des Erblassers in den Nutzungsvertrag mit dem Dienstanbieter eingetreten sind. Hat der Erblasser beispielsweise Kundendaten in einer Cloud gespeichert und sollen diese Daten weiterhin verwaltet werden (etwa um den Geschäftsbetrieb des Erblassers fortzuführen), gelten die damit verbundenen datenschutzrechtlichen Pflichten für die Erben, die diese Daten weiterhin verwalten, fort. Es bedarf dann beispielsweise (weiterhin) einer Rechtsgrundlage für die Datenverarbeitung. Beabsichtigen die Erben z. B. nicht die Fortführung des Erwerbsgeschäfts des Erblassers, sondern die Nutzung der Daten für andere Zwecke, so kann die aktive Weiternutzung auch nicht mehr nach Art. 6 I 1 lit. b DSGVO gerechtfertigt werden. Eine Änderung des Zweckes der Verarbeitung müsste dann im konkreten Fall an den Voraussetzungen des Art. 6 IV DSGVO gemessen werden, d. h. es ist sowohl eine Kompatibilitätsprüfung anzustellen und es ist – nach der hier vertretenen Rechtsansicht – das Vorliegen einer Rechtsgrundlage für die Datenverarbeitung zu prüfen. Bei Fehlen einer dieser Voraussetzungen liegt keine zulässige Datenverarbeitung vor und die Erben sind dann verpflichtet, die Daten Dritter (z. B. von Kunden des Erblassers) zu löschen, Art. 17 I lit. a bzw. lit. b DSGVO.

Zu beachten ist außerdem, dass die DSGVO zahlreiche Pflichten an den Verantwortlichen adressiert. Sind die Erben also als datenschutzrechtlich Verantwortliche anzusehen, müssen sie dementsprechend die datenschutzrechtlichen Pflichten beachten. Dies sind beispielsweise die Informationspflichten aus Art. 13 ff. DSGVO (d. h. die Erben müssen ggf. früher mitgeteilte Informationen berichtigen), das Treffen geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO, Dokumentationspflichten, etc.

2.3.2.3 Folgen bei Weiternutzung

Jedenfalls im Rahmen einer aktiven Weiternutzung eines Accounts bei einem sozialen Netzwerk gelten insoweit Einschränkungen für die in den Vertrag eintretenden Erben, als diese zumindest bei privaten Accounts die Profilseite an ihre Person anpassen oder einen entsprechenden Nachfolgehinweis aufnehmen müssen. Dabei ist insbesondere einer Verletzung des postmortalen Persönlichkeitsrechts des Erblassers vorzubeugen.

2.3.3 Kündigungsrecht

Zu untersuchen ist, ob und wie der oder die Erben berechtigt sind, Online-Vertragsbeziehungen des Erblassers zu kündigen.

Möchte der Erbe ein Nutzerkonto sofort nach dem Erbfall kündigen, so könnte das Kündigungsrecht – erneut analog zu den Grundsätzen für Giroverträge – als Teil der Nachlassabwicklung eingestuft werden. Insofern wäre das Kündigungsrecht bereits vom Erbrecht erfasst, weil kein eigenes Vertragsverhältnis zwischen Erben und Dienstanbieter begründet würde, sondern der Nutzungsvertrag als vom Erblasser abgeleitetes Rechtsverhältnis zu behandeln ist.[55] Dies ergibt dann Sinn, wenn der Erbe nur im Rahmen und zum Zweck der Abwicklung des Nachlasses überhaupt Einsicht in einen Account genommen hat und diesen nach Beendigung der Nachlassgeschäfte ohne eigene Weiternutzung löschen möchte. Der Erbe hatte insoweit keinen Willen und kein Interesse, ein eigenes Vertragsverhältnis zu begründen. Allein die Kündigung oder der Wille hierzu sollte auch nicht zur Begründung eines eigenen Vertragsverhältnisses führen. Vielmehr dient die Kündigung in diesem Fall nur dem Abschluss der Nachlassgeschäfte, indem die nun „nutzlos“ gewordenen Nutzerkonten gelöscht werden.

Erfolgt die Nutzung durch den Erben demgegenüber nicht allein zur Nachlassabwicklung und ist somit der Austausch der Vertragsparteien durch Vertragseintritt des Erben bereits vollzogen, so steht ihm das Kündigungsrecht als eigenes Recht zu. Insofern ergeben sich keine Besonderheiten gegenüber den allgemeinen Regeln zur Kündigung eines eigenen Vertragsverhältnisses.

In den Fällen, in denen der Erbe als datenschutzrechtlich Verantwortlicher zu qualifizieren ist (dazu siehe die Ausführungen oben), ist sicherzustellen, dass betroffene Personen ihre Betroffenenrechte (noch) ausüben können. Gegebenenfalls bietet es sich an, die betroffene Person über die beabsichtigte Kündigung und damit über die beabsichtigte Löschung der sie betreffenden Daten zu informieren, beispielsweise dann, wenn feststeht, dass die betroffene Person die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt und damit einen Anspruch auf Einschränkung der Verarbeitung nach Art. 18 DSGVO hat.[56] In solchen Fällen könnte in Betracht kommen, zunächst mit der Kündigung abzuwarten bzw. entsprechende Daten zu sichern und die betroffene Person hierüber in Kenntnis zu setzen.

[55] *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1922 Rn. 396, 242.
[56] Vgl. *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO Art. 17 Rn. 10 ff., 22 f.

2.4 Zusammenfassung

Der digitale Nachlass ist somit gemäß der erbrechtlichen Vorschriften des BGB grundsätzlich vererblich, und die Erben können vollständig in die Rechtsposition des Erblassers eintreten. Hinsichtlich des erbrechtlichen Übergangs ist dabei zwar nach dem jeweiligen Nachlassgegenstand zu differenzieren. So gehen die Daten auf einem lokalen Speichermedium in anderer Weise über als eine Online-Vertragsbeziehung. Die Regelungen des BGB können die Vererbbarkeit aber abbilden.

Insofern ist nach der hier vertretenen Ansicht keine Anpassung der erbrechtlichen Vorschriften des BGB an etwaige Erfordernisse des digitalen Nachlasses erforderlich, wie dies beispielsweise durch das Gutachten der Datenethikkommission angeregt wird. Danach sollen Nutzerkonten, die besonders persönlichkeitssensitiv sind und daher höchstpersönlichen Charakter haben, grundsätzlich unvererbbar sein und hierfür eine Regelung im BGB geschaffen werden.[57]
Auch eine solche Regelung würde jedoch das – bereits in der Begründung des Urteils des BGH angesprochene – Problem aufwerfen, dass dann eine Abgrenzung von vererbbaren und unvererbbaren Inhalten kaum möglich wäre. Zwar soll die Unvererbbarkeit nach dem Vorschlag nur für „persönlichkeitssensitive“ Nutzerkonten gegeben sein. Hier können die Übergänge zu nicht mehr höchstpersönlichen Inhalten aber fließend sein, sodass durch eine solche Regelung die Gefahr erheblicher Rechtsunsicherheit droht. Zudem fügt sich eine solche Regelung nicht in die sonstigen Regelungen des Erbrechts ein. Analoge Tagebücher, Briefe und Papierfotos sind nach den gesetzlichen Regeln ebenfalls vererbbar, obwohl sie höchstpersönliche Inhalte des Erblassers oder dritter Personen beinhalten können. Insofern eine Differenzierung danach vorzunehmen, ob der höchstpersönliche Inhalt in Papierform oder digital an die Erben übergehen soll, wäre nicht gerechtfertigt. Darüber hinaus steht es dem Erblasser offen, durch eine letztwillige Verfügung den Zugriff der Erben auf solche Nutzerkonten zu verhindern.[58] Sollte im Einzelfall eine andere Beurteilung gerechtfertigt sein, kann dies nach der hier vertretenen Auffassung dadurch gelöst werden, dass hinsichtlich der Vererbbarkeit eine Abwägung anhand des Einzelfalls (ggf. unter Beachtung des TKG, des postmortalen Persönlichkeitsrechts des Erblassers oder der Persönlichkeitsrechte Dritter) erfolgt.

Hierfür ist jedoch keine Änderung des BGB erforderlich und diese daher auch nicht angezeigt. Die geltenden erbrechtlichen Vorschriften können die sich im Rahmen des digitalen Nachlasses stellenden Sachverhalte lösen.

Rechte der Erben am digitalen Nachlass
Der Begriff digitaler Nachlass fasst all das zusammen, was der Verstorbene an nur elektronisch verfügbaren Daten, Vertragsbeziehungen und Vermögen hinterlässt. Dazu gehören (ohne Anspruch auf Vollständigkeit):

[57] Siehe Gutachten der Datenethikkommission der Bundesregierung von Oktober 2019, S. 111.
[58] Hierzu ausführlich in Kapitel 6 auf Seite 175.

- alle auf lokalen Speichermedien (also Computern, Laptops, USB-Sticks oder externen Festplatten) gesicherten Daten
- Daten im Internet oder in Clouds
- Vertragliche Beziehungen des Erblassers zu Dienstanbietern
  - beruflicher oder sozialer Netzwerke
  - Online-Bezahldiensten oder Onlinebanking
  - von Online-Spielen
  - aller sonstigen online abgeschlossenen und abgewickelten Vertragsbeziehungen
- Nutzungsrechte an Musik- oder Sprachwerken, Streamingportalen
- Kryptowährungen

All diese digitalen Nachlassgegenstände gehen grundsätzlich nach den allgemeinen erbrechtlichen Regeln auf die Erben über. Wird ein lokales Speichermedium vererbt, so gehen die darauf gespeicherten Daten zusammen mit dem Speichermedium auf die Erben über. Bei Online-Vertragsbeziehungen gilt zunächst der Grundsatz, dass die Erben in das Vertragsverhältnis zwischen dem Dienstanbieter und dem Verstorbenen eintreten und deshalb dieselben Rechte und Pflichten aus dem Vertrag haben wie der Verstorbene vor ihnen.
Was mit dem Vertrag weiter geschieht, hängt jedoch davon ab, wie die Erben damit verfahren wollen. Dies soll am Beispiel eines Facebook-Profils und eines PayPal-Kontos verdeutlicht werden.
Die Erben führen dann (als vom Verstorbenen abgeleitetes Recht) die ursprüngliche Vertragsbeziehung des Verstorbenen fort, wenn sie sich nur in das Facebook-Profil des Verstorbenen einloggen, um die dortigen Inhalte einzusehen, diese lokal abzuspeichern und das Konto anschließend zu löschen. Entsprechend gilt dies, wenn sich die Erben in das PayPal-Konto des Verstorbenen einloggen, nur mit dem Ziel, Informationen über dort geführte Daueraufträge und ein vorhandenes Guthaben zu erhalten, um anschließend die Daueraufträge zu kündigen, das Guthaben auf ein anderes Konto zu übertragen und den Vertrag mit PayPal zu kündigen. Dies gilt unabhängig davon, ob die beinhalteten Daten rein privat (höchstpersönlich) sind oder einen Vermögenswert haben. Insoweit ergibt sich kein Unterschied, ob die Vererbung analog oder digital erfolgt.

Wollen die Erben dagegen nicht nur Einsicht in die Nutzerkonten nehmen, sondern diese auch selbst als eigene nutzen, führen sie nicht die alte Vertragsbeziehung des Verstorbenen fort, sondern es entsteht ein eigener, neuer Vertrag zwischen dem Dienstanbieter und den Erben. Ist es somit beispielsweise im Interesse der Erben, das Facebook-Profil des Verstorbenen als Erinnerung an diesen (auch über einen begrenzten Zeitraum) weiterzuführen, entsteht ein neuer Vertrag zwischen den oder dem Erben und Facebook. Ähnlich hierzu entsteht dann ein neuer, eigener Vertrag zwischen den Erben und PayPal, wenn diese nach Einsichtnahme eigene Daueraufträge hinzufügen oder Zahlungen im eigenen Interesse (beispielsweise zur Begleichung einer Schuld bei einem Online-Versandhandel) über das PayPal-Konto tätigen. Kündigen die Erben hiernach die Verträge, kündigen sie einen eigenen Vertrag, nicht den fortgeführten Vertrag des Verstorbenen.
Die Grenze zwischen Fortführung des Altvertrages und Begründung eines eigenen Vertrages kann somit dort gezogen werden, wo die Erben nicht mehr nur zu dem Zweck der Nachlassabwicklung, sondern mit eigenem vertraglichen Interesse handeln.
Führen die Erben aber insbesondere einen Social-Media-Account, eine Website oder einen Blog des Verstorbenen weiter, ist unbedingt ein Hinweis darauf zu geben, dass der frühere Nutzer verstorben ist und das Nutzerkonto nun von den Erben weitergeführt wird. Dies kann entweder durch eine Änderung des Nutzernamens geschehen oder durch einen Hinweis auf der Startseite.
Insgesamt müssen hier aber gegebenenfalls Besonderheiten aufgrund der vereinbarten Vertragsbedingungen beachtet werden (dazu ausführlicher im Rahmen des Kapitels 5 auf Seite 115).
Ist die Nutzung von Online-Accounts als datenschutzrechtlich relevant einzustufen, sollten sich die Erben der Rechte und Pflichten, die aus der DSGVO hervorgehen, bewusst sein. Insoweit gelten die allgemeinen datenschutzrechtlichen Vorgaben.

Das Wichtigste in Kürze

- Auch der digitale Nachlass ist vererbbar.
- Die Erben können somit z. B. alle lokal durch den Verstorbenen gespeicherten Daten einsehen, sind aber auch berechtigt, in die Nutzerkonten, die der Verstorbene bei Online-Dienstanbietern (z. B. Social-Media-Accounts, Online-Bezahldienste) geführt hat, Einsicht zu nehmen.
- Die Erben sind auch befugt, Nutzerkonten, die der Verstorbene bei Online-Dienstanbietern geführt hat, weiter zu nutzen, wenn sie dies wünschen.
- Zudem haben die Erben das Recht, diese Nutzerkonten zu kündigen und zu löschen.
- Wenn die Nutzung von Nutzerkonten in den Anwendungsbereich der DSGVO fällt, sind datenschutzrechtliche Vorgaben zu beachten.

3 Digitale Angelegenheiten im Rahmen von Betreuung und Vorsorgevollmacht

Dieses Kapitel untersucht

- die Relevanz digitaler Inhalte für den Fall der Handlungsunfähigkeit eines Nutzers;
- die Rechtslage im Rahmen der Betreuung und bei Vorliegen einer Vorsorgevollmacht;
- welche Befugnisse ein Betreuer als gesetzlicher Vertreter des Nutzers im Hinblick auf den digitalen Bereich hat;
- welche Befugnisse ein Vorsorgebevollmächtigter als freiwillig bestellter Stellvertreter des Nutzers im Hinblick auf den digitalen Bereich haben kann;

3.1 Relevanz der digitalen Angelegenheiten

Eine von der Vererbbarkeit digitaler Werte zu unterscheidende Frage ist, ob der Nutzer berechtigt ist, sich bei der Wahrnehmung seiner Rechte und Pflichten aus den Verträgen mit Dienstanbietern eines Vertreters zu bedienen. Dem Nutzer kann insoweit entweder ein gerichtlich bestellter Betreuer oder ein von ihm privatautonom bestimmter Vorsorgebevollmächtigter zur Seite stehen. Im Ausgangspunkt ist die Situation von Betreuung und Vorsorgevollmacht insofern vergleichbar, als es sich in beiden Fällen um eine (gesetzliche bzw. gewillkürte) Stellvertretung handelt. Allerdings können sich Unterschiede daraus ergeben, dass der Betreuer eine Person ist, derer sich der Staat zur Wahrnehmung seiner Fürsorgeaufgaben bedient und der Vorsorgebevollmächtigte eine vom Betroffenen selbst ausgewählte und mit Kompetenzen ausgestattete Person ist. Auch in diesem Zusammenhang ist die Klärung der rechtlichen Ausgangslage bedeutsam für die Frage, welche Befugnisse in Hinblick auf den digitalen Nachlass privatautonom auf einen Stellvertreter übertragen werden können.

Unterschiede zum Erbfall ergeben sich insoweit, als der noch lebende Nutzer für den Dienstanbieter als Vertragspartner zur Verfügung steht. Der Vertreter tritt hier als dritte Person neben den Nutzer. Zu untersuchen ist nun, wie sich dies auf die rechtliche Bewertung auswirkt.

3.2 Allgemeines

Nicht nur kann ein Nutzer digitaler Angebote oder Dienste versterben, genauso kann der Fall eintreten, dass der Nutzer fürsorgebedürftig wird und seine Angelegenheiten nicht mehr selbst besorgen kann. In diesen Fällen stellt sich die Frage, wie die fürsorgebedürftige Person weiter am Rechtsleben teilhaben und insbesondere ihre digitale Kommunikation fortgeführt werden kann. Insoweit kann der Nutzer entweder vorsorgend privatautonom einen Vertreter bestellen oder – falls es keinen Vorsorgebevollmächtigten gibt (§§ 1896 II 2, 1901c S. 2 BGB) – gerichtlich für den Nutzer ein Betreuer, §§ 1896 ff. BGB, bestellt werden.

Die Frage der Zulässigkeit einer Stellvertretung kann dabei grundsätzlich in demselben Rahmen digitaler Dienste virulent werden, wie bereits in Kapitel 2.1 auf Seite 36 beschrieben wurde. Diesbezüglich ist jedoch stets die Besonderheit zu beachten, dass der Stellvertreter regelmäßig nur dann tätig wird, wenn auch ein Vertretungsbedarf besteht.

3.2.1 Betreuung

Der Begriff der Betreuung meint persönliche rechtliche Betreuung in Form der Rechtsfürsorge für den Betreuten, § 1897 I BGB.[1] Sie kann als privatrechtliches Amt verstanden werden, bei dem der Betreuer seine Aufgaben als gesetzlicher Vertreter fremdnützig (treuhänderisch[2]) wahrnimmt und primär

[1] *Dethloff*, FamR, § 17 Rn. 7.

[2] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 1.

gegenüber dem Betroffenen verantwortlich ist, allerdings von einem staatlichen Organ (Betreuungsgericht) überwacht wird.[3]

Digitale Angelegenheiten

Hierbei kann der Betreuer für verschiedene Aufgabenkreise bestellt werden, soweit dies erforderlich ist, weil eine volljährige Person aufgrund eines Fürsorgebedürfnisses ihre Angelegenheiten ganz oder teilweise nicht selbst besorgen kann, § 1896 I, II BGB.

Dabei kann eine Betreuung auch für die digitalen Angelegenheiten einer Person notwendig werden. Der Begriff soll zunächst erneut nur als Sammelbegriff für den gesamten elektronischen Datenbestand des Betroffenen und sämtliche Rechtsverhältnisse des Betroffenen hinsichtlich informationstechnischer Systeme verstanden werden,[4] hinsichtlich derer ein Fürsorgebedürfnis bestehen kann. Da der Betreuer durch die Betreuungsanordnung aber im Rahmen seines Aufgabenkreises der gesetzliche Vertreter des Betroffenen wird[5] und ihm die zur Durchführung dieser Aufgabe notwendigen Befugnisse zustehen (§ 1902 BGB), müssen sich diese Befugnisse auch auf die digitalen Angelegenheiten des Betroffenen beziehen, soweit sie vom Aufgabenkreis des Betreuers umfasst sind. Die Erforderlichkeit der Betreuung (§ 1896 II BGB) und ein Handlungsbedarf können sich insoweit daraus ergeben, wenn der Betroffene digitale Angebote und Dienste bisher in seinem Alltag genutzt hat, aber nun nicht mehr in der Lage ist, diese (ganz oder teilweise) allein zu beherrschen.

Im Rahmen der Bestimmung der Aufgabenkreise bietet sich dabei zunächst wie nach gängigem Verständnis die Unterteilung in die zwei großen Teilbereiche der Fürsorge an: die persönlichen Angelegenheiten und die Vermögenssorge.[6] Totalbetreuung ist zwar auch hier möglich, soll jedoch die Ausnahme bleiben.[7]

Personenbezogene digitale Angelegenheiten

So kann dem Betreuer im Rahmen der persönlichen Angelegenheiten beispielsweise die Sorge für die Gesundheit, die Aufenthalts- oder Umgangsbestimmung übertragen werden. Letzteres ist gesetzlich ausdrücklich vorgesehen, vgl. § 1908i I 1 BGB i. V. m. § 1632 II BGB und insbesondere dann anzuordnen, wenn sich eine betreute Person krankheitsbedingt gegen belastende Kontakte nicht selbst erwehren kann.[8] Diese belastenden Kontakte können aber nicht mehr nur telefonisch oder persönlich stattfinden, sondern genauso über digitale Kommunikationssysteme, wie (ohne Anspruch auf Vollständigkeit) Instant-Messaging-Dienste, die Chat- oder Nachrichtenfunktion eines Social-Media-Accounts oder eines Online-Spiels sowie via E-Mail.

[3] *Dethloff*, FamR, § 17 Rn. 22.
[4] Vgl. zur ähnlichen Definition im Rahmen des Erbfalls, Kapitel 3.1 auf der vorherigen Seite.
[5] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 18).
[6] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 83.
[7] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 75.
[8] BayObLG, FamRZ 2000, 1524.

Vermögensbezogene digitale Angelegenheiten

Daneben kann sich ein Betreuungsbedarf in Vermögensangelegenheiten auch aus digitalen Angelegenheiten ergeben, wenn diese voraussichtlich anfallen und der Betroffene diese nicht mehr selbst erledigen kann. Dies kann beispielsweise der Fall sein, wenn Bankgeschäfte nicht persönlich in der Bankfiliale, sondern allein digital im Rahmen von Onlinebanking abzuwickeln sind, weil die betroffene Person nicht nur Onlinebanking-Dienste ihrer Filialbank nutzt, sondern ein Konto bei einer reinen Online-Bank (Direktbank) führt.[9]

Insoweit kann der Betreuer entweder für alle Vermögensangelegenheiten oder nur hinsichtlich bestimmter Vermögensmassen bzw. Vermögensgegenstände bestellt werden. Die Reichweite der Anordnung muss zwar grundsätzlich dem Erforderlichkeitsgrundsatz genügen und sollte daher so konkret wie möglich erfolgen,[10] allerdings ist zu beachten, dass eine zu enge Anordnung zu praktischen Umsetzungsschwierigkeiten führen kann.[11] Allein durch die Änderung des Bezugsobjekts könnten daher die Befugnisse des Betreuers enden. Probleme können sich beispielsweise ergeben, wenn sich Vermögen des Betroffenen nicht auf einem Bankkonto, sondern als Guthaben auf einem Online-Bezahldienst-Konto befindet. Diesbezüglich kann die Anordnung des Aufgabenkreises Bankgeschäfte zu eng sein, weil es sich bei einem Online-Bezahldienst (wie z. B. PayPal oder Apple Pay/Google Pay) nicht um eine Bank im klassischen Sinne handelt. Vielmehr gibt beispielsweise PayPal auf seiner Website an, nur eine „offene digitale Bezahlplattform“ zur Verfügung zu stellen, um „Zugang zu Finanzdienstleistungen“ zu schaffen und ihren Kunden zu ermöglichen, „sich auf neue und leistungsfähige Art zu verbinden und Geschäfte zu tätigen“.[12] Dabei ist zwar stets ein Bankkonto oder eine Kreditkarte als Zahlungsquelle zu hinterlegen, allerdings besteht teilweise auch die Möglichkeit, ein eigenes Guthaben auf der Bezahlplattform anzulegen.[13]

Zu beachten ist auch der Fall, dass die fürsorgebedürftige Person ihr Vermögen oder einen Teil ihres Vermögens nicht in einem herkömmlichen Anlagemodell, sondern in Kryptowährungen angelegt hat. Hier gibt es keine ausgebende und kontrollierende Bank oder Institution, sondern die Kryptowährung wird stattdessen von den Nutzern eines offen ausgestalteten und für jeden zugänglichen Peer-to-Peer-Computernetzwerks gemeinsam erschaffen („geschürft“) und verwaltet,[14] sodass sie jedenfalls nicht unter den Aufgabenkreis Bankgeschäfte fallen. Auch wenn die rechtliche Einordnung der Kryptowährungen schwierig und wohl strittig ist, können diese jedenfalls einen Vermögenswert bzw. ein Wirtschaftsgut darstellen,[15] sodass ein Handlungsbedarf durch einen Betreuer grundsätzlich erforderlich werden kann. Aufgrund der starken Kursschwankungen der Kryptowährungen ist der Betreuer aufgrund seiner Pflicht, das Vermögen des Betroffenen zu erhalten, zu sichern und zu vermehren (§ 1908i I 1 BGB i. V. m. §§ 1806 f. BGB) aber möglicherweise gehalten, diese Geldanlage aufzulösen und in eine sichere Kapitalanlage umzulegen.

[9] wie z. B. die comdirect bank AG: https://www.comdirect.de/cms/ueberuns/de/unternehmen/index.html oder die ING-DiBa AG: https://www.ing.de/ueber-uns/unternehmen/standorte.
[10] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 75.
[11] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 121.
[12] Zu PayPal: https://www.paypal.com/de/webapps/mpp/about.
[13] Erneut zu PayPal: https://www.paypal.com/de/webapps/mpp/flexibility.
[14] *Berentsen/Schär*, Bitcoin, S. 69 ff., 110; *Schlund/Pongratz*, DStR 2018, S. 598 (599).
[15] *Schlund/Pongratz*, DStR 2018, S. 598 (601).

Nicht betreuungsrelevante digitale Angelegenheiten

Genauso wenig, wie aber das Schreiben eines Tagebuchs in Papierform eine betreuungsrechtlich relevante Angelegenheit ist, da es insoweit keiner rechtlichen Stellvertretung bedarf,[16] ist auch das Verfassen von privaten Blogs oder Online-Tagebüchern keine Angelegenheit, für die ein Betreuer bestellt werden kann.
Die Erforderlichkeit der Betreuung kann mangels Handlungsbedarfs beispielsweise auch fehlen hinsichtlich der Nutzungsrechte bereits heruntergeladener Dateien (E-Books, Musikdaten, etc.), soweit es nur noch um die rein tatsächliche Nutzung geht. Lädt die fürsorgebedürftige Person jedoch immer weiter kostenpflichtig Dateien herunter und drohen deshalb finanzielle Nachteile, so kann diesbezüglich Betreuungsbedarf bestehen. Ähnliches kann sich ergeben, wenn der Betroffene seine finanziellen Mittel übersteigende Online-Kaufverträge abschließt, an Online-Auktionen teilnimmt oder teure virtuelle Ausrüstung bei Online-Spielen erwirbt. So kann es erforderlich werden, dass der Betreuer gegenüber dem Dienstanbieter kommuniziert, Vertragsangebote des Fürsorgebedürftigen nicht mehr anzunehmen oder diese Kommunikationswege kontrolliert.[17]

Wird der Betreuer gewahr, dass von einer digitalen Angelegenheit ein Betreuungsbedarf ausgeht, ihm diesbezüglich aber keine Befugnisse zustehen, so muss er gegebenenfalls beim Betreuungsgericht die Erweiterung seines Aufgabenkreises anregen.

3.2.2 Vorsorgevollmacht

Hat eine Person eine Vorsorgevollmacht errichtet, geht diese der rechtlichen Betreuung grundsätzlich vor, vgl. §§ 1896 II 2, 1901c S. 2 BGB (Subsidiarität der Betreuung). Im Grundsatz folgt eine Vorsorgevollmacht den allgemeinen Regeln zur Stellvertretung, §§ 164 ff. BGB, mit möglichen Abweichungen aufgrund der Besonderheit, dass die Vorsorgevollmacht für den Fall erteilt wird, dass bestimmte Aufgabenkreise der Personen- oder Vermögenssorge alters- oder krankheitsbedingt übertragen werden sollen.[18]

Grundsätzlich können alle Aufgaben, die auf einen Betreuer übertragen werden können, auch durch Vorsorgevollmacht übertragen werden,[19] so auch die Kompetenzen zu Aufenthaltsbestimmung bzw. Umgangsregelung.[20] Somit können bei entsprechender Bevollmächtigung auch die Befugnisse hinsichtlich der soeben beschriebenen digitalen Angelegenheiten im Grundsatz privatautonom durch einen Vorsorgebevollmächtigten wahrgenommen werden. Insoweit kann der Vollmachtgeber selbst beurteilen, ob er einen Fürsorgebedarf für erforderlich hält und inwieweit er dem Bevollmächtigten Befugnisse einräumt. Soweit der Vorsorgebevollmächtigte durch die Vollmacht legitimiert ist, kann er als gewillkürter Stellvertreter des Betroffenen im Rechtsverkehr auftreten.

[16] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 101.
[17] Siehe hierzu sogleich.
[18] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK, BGB § 1896 Rn. 223 ff.
[19] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 256.
[20] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 107; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 176; *Kropp*, FPR 2012, S. 9.

Ist die Vorsorgevollmacht einmal wirksam erteilt, hat eine danach eintretende Geschäftsunfähigkeit des Vollmachtgebers in der Regel keine Auswirkungen auf die Wirksamkeit der Vollmacht (§ 168 S. 1, § 672 S. 1, § 675 I BGB), da es häufig gerade Sinn und Zweck der Vorsorgevollmacht ist, dem Vollmachtgeber trotz des Verlusts rechtlicher Handlungsfähigkeit weiter als Rechtssubjekt die Teilnahme am Rechtsverkehr zu ermöglichen – auch wenn dies nunmehr vertreten durch den Vorsorgebevollmächtigten erfolgt.[21]

Die privatautonome Vorsorgevollmacht stößt jedoch dort an ihre Grenzen, wo der Bevollmächtigte die Aufgabe nicht ebenso gut wie ein rechtlicher Betreuer wahrnehmen kann (qualitativer Vergleich, vgl. hierzu § 1896 II 2 BGB). Dies ist beispielsweise der Fall, wenn bestimmte Maßnahmen nicht durch privatautonome Stellvertretung übertragen werden können, wie amtsähnliche Befugnisse (z. B. eigene Antrags-, Beschwerderechte im Namen des Betreuers) oder die Anordnung eines Einwilligungsvorbehalts, die nur durch ein Gericht erfolgen kann, § 1903 BGB.[22] Von der nun beschränkt geschäftsfähigen Person vorgenommene und daher schwebend unwirksame Rechtsgeschäfte können nur durch Einwilligung eines Betreuers zur Wirksamkeit gelangen. Die betroffene Person kann aber zumindest dadurch auf diese Situation Einfluss nehmen, indem sie eine von ihr ausgewählte Person als Betreuer vorschlägt, § 1894 IV 1 BGB.[23] Dies gilt auch für Rechtsgeschäfte, die der Vollmachtgeber online abschließt.

3.3 Umfang der Befugnisse

Soweit ein Betreuer oder Vorsorgebevollmächtigter hinsichtlich der digitalen Angelegenheiten als Vertreter bestellt ist, müssen ihm auch ausreichende Befugnisse zustehen, um die diesbezüglichen Aufgaben ordnungsgemäß ausüben zu können. Erneut bietet sich hinsichtlich des Umfangs der Befugnisse eine Differenzierung zwischen dem bloßen Einsichtsrecht, dem aktiven Nutzungsrecht und dem Recht zur Kündigung an.
Diese Frage kann einerseits die digitalen Kommunikationswege betreffen, über welche die fürsorgebedürftige Person ihre geschäftliche oder private Kommunikation vollzieht, wie im Rahmen der Nutzungsverträge mit Anbietern sozialer bzw. beruflicher Netzwerke oder E-Mail-Accounts. Daneben können aber auch sonstige Kommunikationswege betroffen sein, wie die Chat-Funktion bei Online-Spielen oder in Apps (wie WhatsApp oder Telegram) sowie in Verkäuferportalen (wie eBay, die ebenfalls eine Nachrichtenfunktion haben). Einsichts- oder Nutzungsbefugnisse könnten dem gesetzlichen oder gewillkürten Vertreter aber beispielsweise auch hinsichtlich lokaler Speichermedien oder im Rahmen von Onlinebanking oder Online-Bezahldiensten zustehen.

[21] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 60 f.; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 237.
[22] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 229.
[23] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (16).

3.3.1 Einsichtsrecht

3.3.1.1 Betreuung: Familienrechtliche Betrachtung

Zu untersuchen ist zunächst, ob der rechtliche Betreuer befugt ist, Einsicht in digitale Inhalte der betroffenen Person zu nehmen und insbesondere an sie gerichtete Nachrichten zu lesen.

Gemeinsame Durchsicht/Weiterleitung

Wie bei analoger Post ist zunächst die Situation denkbar, dass die (einwilligungsfähige) betreute Person die Öffnung und Sichtung der Post durch den Betreuer selbst gestattet oder diese zunächst selbst öffnet und anschließend an den Betreuer weitergibt bzw. weiterleitet.[24] Daneben kann (schriftlich) eingehende Post zunächst dem Betreuten selbst ausgehändigt und dann (ggf. im Beisein der betroffenen Person) gesichtet und gelesen werden.[25] Dies kann auf die digitale Kommunikation der betroffenen Person übertragen werden. Auch hier sind ein gemeinsames Einloggen, Sichten und Lesen mit dem Betreuer oder das eigenständige Lesen durch die betroffene Person mit Weiterleitung an den Betreuer denkbar und möglich.
Mit Einwilligung des Betroffenen ist der Betreuer auch ohne gesonderte Anordnung befugt, bereits geöffnete Post durchzusehen, um sich beispielsweise zu Beginn seiner Tätigkeit einen Überblick über seine Betreuungsaufgaben zu verschaffen.[26] Dies umfasst nach richtigem Verständnis der Befugnisse nicht nur Briefpost, sondern auch bereits geöffnete E-Mails, die der Betroffene auf einem lokalen Speichermedium gesichert hat.

Fernmeldekontrolle, § 1896 IV BGB

Ist aber nicht sichergestellt, dass die betroffene Person die Post (zuverlässig) weiterleitet bzw. in der Lage ist, die Post selbst zu öffnen, den Inhalt einzuordnen und zu verstehen oder mit dem Inhalt angemessen umzugehen, muss die Anordnung einer Post- bzw. Fernmeldekontrolle durch das Betreuungsgericht erwogen werden.

Eine solche Kontrollbefugnis des Betreuers hinsichtlich des Post- und Fernmeldeverkehrs des Betreuten ist in § 1896 IV BGB geregelt. Danach kann die Entscheidung über den Fernmeldeverkehr und über die Entgegennahme, das Öffnen und das Anhalten der Post des Betreuten vom Aufgabenkreis des Betreuers umfasst sein, wenn dies ausdrücklich durch das Betreuungsgericht angeordnet wurde. „Entgegennahme und Öffnen“ der Post betreffen insoweit nur die eingehende Post. „Anhalten“ meint sowohl eingehende als auch von der betreuten Person versandte Post.[27]

Die Entscheidung über den Fernmeldeverkehr und Befugnisse hinsichtlich der Post des Betroffenen ermöglichen nicht nur die Kontrolle des analogen Brief- und Postverkehrs, sondern auch des mobilen

[24] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 20 a. E.).
[25] OLG München, FamRZ 2008, 89; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 292; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 280.
[26] *Deinert/Lütgens*, BtPrax 2009, S. 212 (214).
[27] *Deinert/Lütgens*, BtPrax 2009, S. 212 (213).

Telefon-, E-Mail- und SMS-Verkehrs sowie der Nutzung von Social Media oder beruflich genutzten elektronischen Netzwerken[28] und allen sonst möglichen digitalen Kommunikationswegen.

Insbesondere wenn der Betreuer bestellt ist, zum Schutz der fürsorgebedürftigen Person deren Umgang zu bestimmen, kann eine Kontrolle von privaten, digitalen Kommunikationswegen Bedeutung erlangen. Dabei kann auch die Kontrolle von Instant-Messaging-Apps (z. B. WhatsApp, Telegram) angezeigt sein. Kommuniziert die betroffene Person mit (Online-)Bekanntschaften über die Chat-Funktion von Online-Spielen, so kann, wenn hierfür ein Bedarf besteht, auch dieser Kommunikationsweg kontrolliert werden.

Ist der Betreuer zur Vermögenssorge bestellt, ist gegebenenfalls auch die Kontrolle von Verkaufsportalen (wie eBay, Shpock, Kleiderkreisel) oder Online-Bezahldiensten zu bedenken, um den Betroffenen vor unsinnigen oder selbstschädigenden Bestellungen zu schützen.

Voraussetzungen der Anordnung

Es ist im Einzelfall zu bestimmen, hinsichtlich welcher Kommunikationswege die Kontrolle durch den Betreuer notwendig erscheint. Der rechtliche Betreuer ist dabei nicht allein aufgrund der Übertragung eines anderen Aufgabenkreises – wie Vermögenssorge, Gesundheitssorge, Erledigung persönlicher Angelegenheiten oder sogar im Rahmen der Totalbetreuung – befugt, die persönliche Kommunikation und Korrespondenz der betroffenen Person eigenständig zu kontrollieren. Allerdings stellt die Kontrollbefugnis keinen eigenen Aufgabenkreis oder eine Erweiterung der Aufgaben des Betreuers dar, sondern sie ist stets Annexkompetenz eines anderen Aufgabenkreises, die dem Betreuer die sachgerechte Erledigung des ihm übertragenen Aufgabenkreises ermöglichen soll. Die in § 1896 IV BGB beschriebene Befugnis ist stets ausdrücklich durch das Betreuungsgericht anzuordnen. Sie stellt aufgrund des Eingriffs in Art. 10 GG und Art. 2 I GG (Brief-, Post- und hier insbesondere Fernmeldegeheimnis[29] sowie informationelle Selbstbestimmung) eine besonders gravierende Maßnahme dar und muss daher der strikten Einhaltung des Verhältnismäßigkeitsgrundsatzes genügen.[30] Insbesondere muss die Anordnung erforderlich sein (vgl. auch § 1896 II BGB), um sicherzustellen, dass der Betreuer seine Aufgaben zum Wohl der betroffenen Person erfüllen kann, oder dass keine Rechtsgüter der betroffenen Person gefährdet werden, wobei das Gesetz für den Prüfungsmaßstab selbst keine Anhaltspunkte liefert.[31] Jedenfalls müssen sich im Einzelfall konkrete Anhaltspunkte dafür ergeben, dass die betroffene Person ihre private bzw. geschäftliche Kommunikation nicht mehr selbst wahrnehmen kann und eine Abwägung der betroffenen Rechtsgüter im Einzelfall erfolgen. Die Erforderlichkeit ist wohl zu bejahen, wenn die betroffene Person nicht mehr in der Lage ist, „die für sie bestimmte Post [zu] bearbeiten oder auch nur [zu] begreifen“[32] und dadurch der Betreuer verhindert wäre, wichtige finanzielle bzw. allgemein seinen Aufgabenkreis betreffende Angelegenheiten zu besorgen.[33] Ersteres

[28] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 287; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 281.
[29] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 20).
[30] BayObLG, FamRZ 1997, 244 (245); *Dethloff*, FamR, § 17 Rn. 25; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 278 f.
[31] BayObLG, FamRZ 1997, 244 (245).
[32] BayObLG, FamRZ 2002, 1225 (1226).
[33] *Jurgeleit*, in: Jurgeleit (Hrsg.), Betreuungsrecht Handkommentar, § 1896 Rn. 186.

ist gegebenenfalls durch ein Sachverständigengutachten zu klären.[34]

Ein Fürsorgebedürfnis ist in diesem Rahmen nicht schon deshalb zu bejahen, um störendes Verhalten des Betroffenen gegenüber Dritten zu unterbinden, da die Betreuung eine Hilfestellung für die betroffene Person darstellen soll. Daher ist die Anordnung in diesem Fall nur dann erforderlich, wenn der Betroffene „vor den berechtigten Reaktionen und Maßnahmen Dritter zu schützen [ist], die als Folge seines Verhaltens zu erwarten sind".[35] Dies wurde zur Kontrolle des Fernmeldeverkehrs in einem Fall bejaht, in dem die betroffene Person private Dritte wiederholt telefonisch belästigt hat, um sie vor wahrscheinlichen gerichtlichen Unterlassungs- oder Schadensersatzklagen sowie Ermittlungsverfahren wegen Körperverletzung oder Stalking zu schützen.[36] Ähnliches muss gelten, wenn die fürsorgebedürftige Person via Instant-Messaging-, Social-Media- oder E-Mail-Account belästigende Nachrichten oder Bilder versendet. Denkbar ist jedoch auch, dass die betroffene Person aufgrund einer psychischen Krankheit sogar in öffentlichen Blog-Einträgen oder über eine Website beleidigende Inhalte über eine Person teilt. Droht dies zu Nachteilen für den Betroffenen zu führen, muss der Betreuer berechtigt sein, auch die ausgehenden Nachrichten zu kontrollieren und dies zu unterbinden.

Jedenfalls nicht erforderlich ist die Anordnung, wenn – wie anfangs bereits beschrieben – die (einwilligungsfähige) betreute Person die Öffnung und Sichtung der Post durch den Betreuer selbst gestatten kann oder wenn im Einzelfall sichergestellt ist, dass die betroffene Person die digitale Post selbst öffnet und an den Betreuer weitergibt.[37] Daneben ist wieder denkbar, dass als milderes Mittel die eingehende Post der fürsorgebedürftigen Person zunächst ausgehändigt wird, vor allem E-Mails also zunächst an sie direkt gesendet werden, und dann (ggf. in ihrem Beisein) gesichtet und gelesen wird, anstatt der betroffenen Person die digitale Kommunikation von vornherein vorzuenthalten.[38]

Erforderlich ist, dass im Zeitpunkt der Entgegennahme der (sowohl analogen als auch digitalen) Post durch den Betreuer diese Handlung von seiner gesetzlichen Vertretungsmacht gedeckt war. Durch nachträgliche Erweiterung des Aufgabenkreises kann keine Heilung eintreten, da die maßgebliche Handlung durch den Akt der Entgegennahme der Post oder Kommunikation abgeschlossen ist.[39]

Ausübung durch den Betreuer

Nichtsdestoweniger befugt die Erteilung einer „Postvollmacht" den Betreuer nicht zur Entgegennahme und Sichtung sämtlicher Kommunikation an die betreute Person. Vielmehr ist der Betreuer nur für die Öffnung derjenigen Post zuständig, die auch seinen Aufgabenkreis betrifft und sich innerhalb des ihm übertragenen Aufgabenkreises befindet.[40] Hat ein Betreuer die Aufgabe, den Aufenthalt und den Umgang der betroffenen Person zu bestimmen (und gegebenenfalls den Umgang mit bestimmten

[34] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 168.
[35] OLG München, FamRZ 2008, 1476.
[36] OLG München, FamRZ 2008, 1476.
[37] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 20 a. E.).
[38] OLG München, FamRZ 2008, 89; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 292; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 280.
[39] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 26).
[40] OLG Karlsruhe, NJW-RR 2015, 1031 (1033 Rn. 21 f.); *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 292; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 280.

Personen zu verhindern), so kann dem Betreuer in dem zur Erfüllung dieser Aufgabe notwendigen Umfang die Postkontrollbefugnis zustehen.[41] Ist dem Betreuer aber lediglich die Vermögenssorge übertragen, so ist er auf keinen Fall befugt, die private Kommunikation der betreuten Person zu kontrollieren.

Hinsichtlich des Einsichtsrechts ist daher nicht generell – wie im Rahmen des Erbfalls angedacht – zwischen vermögensrechtlichen oder (höchst)persönlichen Inhalten zu differenzieren. Die Differenzierung des Einsichtsrechts erfolgt sinnvollerweise vielmehr anhand des Aufgabenkreises des Betreuers. Ist er für die persönlichen Angelegenheiten bestellt, ist er auch befugt, private Nachrichten zu lesen, nicht aber die geschäftlichen oder vermögensrelevanten Korrespondenzen der fürsorgebedürftigen Person.

In der Regel wird der Betreuer somit – die ordnungsgemäße Ausübung seiner Befugnisse vorausgesetzt – von vornherein nur von der seinen Aufgabenkreis betreffenden Kommunikation Kenntnis erlangen. Trotzdem kann es zu praktischen Umsetzungsschwierigkeiten kommen, beispielsweise wenn allein durch den Absender oder die Betreffzeile nicht ersichtlich ist, welchen Inhalt eine Nachricht hat. Nach wohl überwiegender Meinung darf der Betreuer aber im Zweifel Post, die ungeöffnet nicht zugeordnet werden kann, öffnen.[42] Entsprechend darf der Betreuer eine E-Mail oder eine sonstige digital versendete Nachricht im Zweifel öffnen, wenn ihr Inhalt anhand der ungeöffneten Nachricht nicht ohne Weiteres erkennbar ist. Allerdings muss der Betreuer gegebenenfalls nachweisen, zumindest den Versuch unternommen zu haben, nur die seinen Aufgabenkreis betreffende Kommunikation zu überwachen. Erlangt er daneben von anderen Inhalten Kenntnis, stehen ihm diesbezüglich jedenfalls keine Befugnisse zu. Auch wenn der Betreuer nicht für jede einzelne Maßnahme der gerichtlichen Genehmigung bedarf, sondern die einmalige gerichtliche Ermächtigung betreffend den Aufgabenkreis ausreicht, so stellen willkürliche Eingriffe in Art. 10 I, 2 I GG schwere Rechtsverletzungen dar. Hiergegen hat das Betreuungsgericht gegebenenfalls einzuschreiten, vgl. § 1908i I 1 i. V. m. § 1837 BGB.[43]

Ist anzunehmen, dass von einem gewissen Medium keine den Aufgabenkreis des Betreuers betreffende Gefährdung droht, scheidet die gesamte Kontrolle dieses Mediums aus,[44] da insoweit die Erforderlichkeit fehlt. Die Selbstbestimmung der betroffenen Person ist so weit wie möglich zu gewährleisten.[45]

Nutzt die unter rechtlicher Betreuung stehende Person also beispielsweise einen Social-Media-Account zu rein privaten Zwecken der persönlichen Kommunikation, und ist der Betreuer allein zur Vermögenssorge bestellt, so scheidet eine Kontrolle bzw. ein Zugang des Betreuers zu diesem Account von vornherein aus. Handelt es sich jedoch um einen E-Mail-Account, über den sowohl persönliche

[41] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 288.
[42] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 292; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 280.
[43] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 283.
[44] *Schmidt-Recla* in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 292; *Schneider* in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 280.
[45] OLG München, FamRZ 2008, 89.

als auch geschäftliche Kommunikation erfolgt, ist dem Betreuer zunächst Zugang zu dem E-Mail-Account zu gewähren, wenn dies zur Wahrnehmung seiner Aufgaben zum Wohl der betroffenen Person erforderlich ist. Die Beurteilung, ob E-Mails seinen Aufgabenkreis betreffen, obliegt dann dem Betreuer im Rahmen sachgemäßer Prüfung. Ist allein anhand des Absenders und des Betreffs nicht ersichtlich, ob die Nachricht für den Aufgabenkreis des Betreuers relevant ist, so muss der Betreuer auch hier im Zweifel berechtigt sein, die Nachricht zu überprüfen. Dies gilt wohl selbst dann, wenn der Betreuer auf diese Weise von Umständen Kenntnis erhält, die nicht seinen Aufgabenkreis oder sogar private Informationen betreffen, weil eine Nachricht sowohl geschäftlichen als auch persönlichen Inhalt hat, der Betreuer aber nur für einen der Aufgabenkreise bestellt ist.

Unabhängig von diesen Befugnissen zur Fernmeldekontrolle ist einem Betreuer mit dem entsprechenden Aufgabenkreis zur Vermögenssorge Zugang zu den Onlinebanking-Portalen des Betroffenen und den dort geführten Girokonten zu gewähren. Insoweit kann im Ausgangspunkt hinsichtlich des Nachweises der Berechtigung und dem Zugang zu Konten bzw. Depots der fürsorgebedürftigen Person nichts anderes gelten, als wenn diese ihre Konten bei einer Filialbank führt. Gleiches muss entsprechend auch für Online-Bezahldienste, die nicht von einer Bank geführt werden, gelten.

3.3.1.2 Betreuung: datenschutzrechtliche Betrachtung

Nach der hier vertretenen Rechtsauffassung dürften sich regelmäßig keine datenschutzrechtlichen Bedenken gegen ein Einsichtsrecht ergeben, da neben dem Einholen einer Einwilligung nach Art. 6 I 1 lit. a DSGVO jedenfalls eine Rechtfertigung der Datenverarbeitung nach Art. 6 I 1 lit. e bzw. Art. 9 II lit. c DSGVO in Betracht kommt. Im Einzelnen ist die Einschlägigkeit der jeweiligen Rechtfertigungsnormen der DSGVO in der Literatur umstritten, und es fehlt noch an gefestigter Rechtsprechung zu dem Thema.

Datenverarbeitungen bedürfen zu ihrer Rechtmäßigkeit, wie jede Verarbeitung personenbezogener Daten, der Einwilligung nach Art. 6 I 1 lit. a DSGVO bzw. einer gesetzlichen Erlaubnis. Liegt ein gesetzlicher Erlaubnisgrund vor, kommt es auf das Vorliegen einer wirksamen Einwilligung nicht mehr an. Aus praktischer Sicht würde das Vorliegen eines gesetzlichen Erlaubnisgrundes mehr Rechtssicherheit bieten als die Abgabe einer Einwilligung, da bei letzterer die Gefahr besteht, unwirksam zu sein oder widerrufen zu werden.[46] Als praxisgerechte Lösung kommt vielmehr Art. 6 I 1 lit. e DSGVO in Betracht. Danach ist die Datenverarbeitung dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Ein solches öffentliches Interesse liegt bei der Übernahme einer Betreuung vor, da die Betreuung das Ziel hat, Menschen mit Behinderung oder Erkrankungen weiterhin die Teilnahme am gesellschaftlichen Leben zu ermöglichen, was eine Aufgabe

[46] Zu der Frage der generellen Erforderlichkeit der Einholung einer Einwilligung durch Berufsbetreuer vertritt der Bundesverband freier Berufsbetreuer e.V. die Ansicht, dass eine Einwilligung aufgrund des in vielen Fällen bestehenden Ungleichgewichts zwischen Betreuer und Betreutem sowie der Widerrufbarkeit der Einwilligung keine rechtssichere Legitimation zur Datenverarbeitung darstellt: https://btdirekt.de/thema/datenschutz.html Überschrift „Datenschutz im Betreuerbüro – Aktuelle Informationen Teil 7“.

darstellt, die im öffentlichen Interesse liegt.[47] Dies gilt auch für die im Aufgabenkreis des Betreuers liegende Kontrolle der Kommunikation. Da eine solche Befugnis einen gravierenden Eingriff in die Grundrechte des Betreuten darstellt, ist es erforderlich, dass die in § 1896 BGB normierten gesetzlichen Voraussetzungen für die Anordnung vorliegen und die Anordnung verhältnismäßig ist.[48]

Kommt es, wie beispielsweise bei der Gesundheitssorge, zu einer Verarbeitung besonderer Kategorien personenbezogener Daten (wie Gesundheitsdaten), kann eine Erlaubnis nach Art. 9 II lit. c DSGVO vorliegen. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben. Lebenswichtige Interessen im Sinne dieser Vorschrift sind auch schon dann zu bejahen, wenn es generell um einen besonderen Gesundheitsschutz geht.[49] Je nach Fallkonstellation, d. h. abhängig vom Aufgabenkreis des Betreuers und der damit erforderlichen Post- und Fernmeldekontrolle, kommen andere Rechtfertigungsgründe in Betracht. So kann insbesondere für die Geltendmachung sämtlicher sozialrechtlicher Ansprüche im Interesse des Betreuten auf Art. 9 II lit. f DSGVO verwiesen werden, wonach eine Datenverarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Generell bleibt jedoch anzumerken, dass es noch an einschlägiger Rechtsprechung zu der Thematik fehlt. Insoweit bleibt abzuwarten, welchen Weg die Rechtsprechung bei der Auslegung der datenschutzrechtlichen Vorschriften beschreiten wird. Sollten die in Art. 6 und 9 DSGVO aufgeführten gesetzlichen Erlaubnistatbestände nicht ausreichen, bliebe als letzter Ausweg noch eine (mit Rechtsunsicherheit behaftete, vgl. oben) Einwilligung durch den Betreuten oder – bei Fehlen der erforderlichen Einwilligungsfähigkeit – durch den Betreuer selbst.[50] So hat das AG Gießen[51] eine (nach seiner Ansicht erforderliche) Einwilligung des Betreuers gegenüber sich selbst nicht aufgrund des Verbots des Insichgeschäfts nach § 181 BGB scheitern lassen, da die für eine solche Konstellation an sich vorgesehene Bestellung eines Ersatzbetreuers zu einem Kurzschluss führe. Dessen Tätigwerden müsse nämlich wiederum durch eine Einwilligung abgedeckt sein, so auch das Tätigwerden eines Ersatz-Ersatzbetreuers, usw. Daher solle der Betreuer selbst innerhalb seines Aufgabenkreises einwilligungsbefugt sein.[52]

In Bezug auf die datenschutzrechtlichen Belange von Kommunikationspartnern des Betreuten können die obigen Ausführungen hinsichtlich der datenschutzrechtlichen Rechtfertigung eines Zugangs durch die Erben auf Online-Accounts des Erblassers auf die vorliegende Konstellation übertragen werden.[53] Insoweit kann regelmäßig von einer Rechtfertigung über Art. 6 I 1 lit. f DSGVO ausgegangen werden.

[47] *Buchner*, FamRZ 2019, 665 (669).
[48] Hierzu vgl. oben unter „ Voraussetzungen der Anordnung“.
[49] *Buchner*, FamRZ 2019, 665 (669).
[50] *Buchner*, FamRZ 2019, 665 (670).
[51] *AG Gießen*, Beschluss vom 16. Juli 2018 – 230 XVII 381/17 G –, juris.
[52] *AG Gießen*, Beschluss vom 16. Juli 2018 – 230 XVII 381/17 G –, juris.
[53] Vgl. *Buchner*, FamRZ 2019, 665 (670).

3.3.1.3 Vorsorgevollmacht: Familienrechtliche Betrachtung

Im Rahmen der Vorsorgevollmacht hängt das Bestehen oder der Umfang eines Einsichtsrechts zunächst davon ab, inwiefern der Vollmachtgeber seinem Stellvertreter diese Befugnisse privatautonom übertragen hat. Jedenfalls ist auch hier möglich, dass Vollmachtgeber und Bevollmächtigter Kommunikationsinhalte gemeinsam sichten und öffnen bzw. der Vollmachtgeber die durch ihn geöffnete relevante digitale Post an seinen Bevollmächtigten weiterleitet oder ihm Zugang zu einem lokalen Speichermedium verschafft.

Übertragung der Befugnisse aus § 1896 IV BGB

Genauer zu untersuchen ist aber die Frage, inwieweit dem Bevollmächtigten die Befugnisse nach § 1896 IV BGB durch den Vollmachtgeber privatautonom übertragen werden können, also insbesondere, inwiefern der Bevollmächtigte den Fernmeldeverkehr überwachen sowie Post anhalten bzw. öffnen oder die Herausgabe der Post von Dritten verlangen darf. Hier wird mit einem Erst-Recht-Schluss vertreten, dass, wenn schon die Unterbringungsbefugnis auf den Vorsorgebevollmächtigten übertragen werden kann, erst recht die Übertragung des weniger gravierenden Eingriffs der Post- und Fernmeldeverkehrsüberwachung möglich sein muss.[54] Von der Gestaltungsbefugnis des Vollmachtgebers ist es somit jedenfalls umfasst, die Post- oder Fernmeldekontrolle ausdrücklich in der Vollmachtsurkunde anzuordnen, was aus Beweisgründen und um Konflikte von vornherein zu verhindern zu empfehlen ist.

Strittig ist jedoch, ob der Vorsorgebevollmächtigte zur Kontrolle der Kommunikation befugt ist, wenn dies nicht ausdrücklich in der Vorsorgevollmacht geregelt ist.

e. A.: Ausdrückliche Anordnung nicht zwingend erforderlich

Dabei wird die Ansicht vertreten, dass § 1896 IV BGB auf die Vorsorgevollmacht nicht (entsprechend) anzuwenden sei.[55] Die Rechtsstellung von Betreuer und Vorsorgebevollmächtigtem sei grundsätzlich unterschiedlich zu beurteilen. Die Bestellung eines Betreuers ist staatliche Fürsorgemaßnahme für die betroffene Person. Der Staat bedient sich des Betreuers als Privatperson zur Erfüllung seiner öffentlichen Fürsorgeaufgaben, sodass Betreuerhandeln an den für den Staat geltenden Grundrechtsschranken zu messen sei. Um in die Grundrechte der betreuten Person (hier insbesondere Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung, Art. 10, 2 I GG) eingreifen zu dürfen, bedarf der Betreuer daher einer speziellen Ermächtigung.[56] Im Gegensatz hierzu sei ein Vorsorgebevollmächtigter ein privatautonom legitimierter (gewillkürter) Stellvertreter des Vollmachtgebers, der den staatlichen Grundrechtsschranken grundsätzlich nicht unmittelbar unterliegt. Der Vorsorgebevollmächtigte leitet seine Befugnisse – auch im grundrechtsrelevanten Bereich – nicht aus staatlicher Bestellung ab, sondern allein aus der gewillkürten Ermächtigung durch den Vollmachtgeber. Im Gegensatz zur gesetzlichen Betreuerbestellung ist die Erteilung einer Vollmacht Ausdruck von Selbst-

[54] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 259.

[55] *Müller-Engels*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 1896 Rn. 53; *Müller*, DNotZ 2015, S. 403 (407 f.); DNotI-Report 2013, S. 148 (149).

[56] Grundlegend BVerfG, NJW 1960, 811 (813); BGH, NJW 2001, 888 (890).

nicht Fremdbestimmung, weshalb auch die gesetzliche Einschränkung des § 1896 IV BGB (weder direkt noch analog) für den Vorsorgebevollmächtigten gelte.[57]

Dafür spreche auch, dass eine entsprechende Einschränkung für die Vorsorgevollmacht im Gesetz nicht vorgesehen sei. An anderer Stelle – namentlich für ärztliche Maßnahmen und Unterbringungsmaßnahmen – ist das Erfordernis der ausdrücklichen Übertragung gesetzlich demgegenüber vorgesehen, vgl. § 1904 V 2 BGB und § 1906 V 1 BGB.[58] Im Umkehrschluss ergebe sich daraus, dass aufgrund des Fehlens einer entsprechenden Spezialregelung für die Post- und Fernmeldekontrolle eine ausdrückliche Ermächtigung nicht notwendig ist.[59]

Insbesondere wenn die Vorsorgevollmacht als Generalvollmacht – die auch zur Entgegennahme von Erklärungen berechtigt – erteilt wurde, sei der Vorsorgebevollmächtigte (aufgrund der umfassenden Wirkung insbesondere notarieller General- oder Vorsorgevollmachten) ohne ausdrückliche Ermächtigung berechtigt, von den zuständigen Poststellen oder sonstigen Dritten die Herausgabe der an die betroffene Person adressierten Post zu verlangen.[60]

Konkludente Übertragung nur in engen Grenzen

Zwar ist diese Argumentation im Grundsatz richtig. Allerdings ist darauf zu achten, dass dem Bevollmächtigten nicht vorschnell Befugnisse zugestanden werden, die der Vollmachtgeber so nicht übertragen wollte. Zwar mag der gewillkürte Stellvertreter nicht in gleicher Weise (direkt) grundrechtlich gebunden sein, wie der gesetzliche Vertreter. Trotzdem ist bei einer eigenständigen Post- oder Fernmeldekontrolle des Bevollmächtigten, also dem Anhalten und Öffnen der Post ohne Beteiligung des Vollmachtgebers im Einzelfall, der grundrechtsrelevante Bereich der Art. 10, 2 I GG betroffen und insoweit auch der Bevollmächtigte als Privatperson jedenfalls mittelbar gebunden. Der Bevollmächtigte darf hier deshalb nur tätig werden, wenn dies dem Willen des Vollmachtgebers entspricht. Selbst wenn wohl eine ausdrückliche Ermächtigung entsprechend § 1896 IV BGB nicht zwingend erforderlich ist, ist zumindest zu verlangen, dass sich ein entsprechender Wille (angedeutet oder durch Auslegung) aus der Urkunde oder dem sonstigen Verhalten des Vollmachtgebers ergibt.[61] Kann ein entsprechender Wille im Rahmen einer Generalvollmacht möglicherweise in engen Grenzen noch konkludent angenommen werden, ist jedenfalls bei nur beschränkter Vollmacht der Wille des Vollmachtgebers eingehend zu erforschen. Insoweit kann auch im Rahmen der möglichst zu wahrenden Selbstbestimmung des Vollmachtgebers eine Abwägung notwendig werden, ob seinem Willen besser dadurch Rechnung getragen werden kann, dass der Bevollmächtigte möglichst weitgehende Befugnisse erhält, oder ein gerichtlich bestellter – und dann auch gerichtlich kontrollierbarer – Betreuer die Aufgabe wahrnehmen soll.

Um zu verhindern, dass insoweit über Umfang und Reichweite der Vollmacht zunächst Streit entsteht, – insbesondere weil sich ein Dienstanbieter weigert, Zugang zu einem Account zu gewähren – ist es

[57] DNotI-Report 2013, S. 148 (149).
[58] *Müller*, DNotZ 2015, S. 403 (407 f.); DNotI-Report 2013, S. 148 (149).
[59] DNotI-Report 2013, S. 148 (149).
[60] *Müller*, DNotZ 2015, S. 403 (408).
[61] Allgemein zur Ermittlung des Umfangs einer Vollmacht durch Auslegung, *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 56.

daher nichtsdestoweniger zu empfehlen, die Befugnis des Bevollmächtigten zur Fernmeldekontrolle in der Vorsorgevollmacht ausdrücklich anzuordnen, wenn diese gewünscht ist.

Daneben ist die ausdrückliche Bevollmächtigung zur Post- und Fernmeldekontrolle auch deshalb zu empfehlen, da für den Vorsorgebevollmächtigten ohne wirksame Vollmacht die Gefahr besteht, sich nach den §§ 202 ff. StGB strafbar zu machen. Zwar ist § 202 StGB nicht auf rein digital gesendete und gespeicherte Nachrichten anwendbar, da es insoweit an der notwendigen Verkörperung wie bei einem verschlossenen Brief oder Schriftstück fehlt.[62] In Betracht kommt insoweit aber eine Strafbarkeit nach den §§ 202a–c StGB, beispielsweise wenn der Vertreter auf einem lokalen Speichermedium (zumindest vorübergehend, ausreichend ist auch die Sicherung im Arbeitsspeicher eines Rechners) gesicherte Nachrichten einsieht, die vor unberechtigtem Zugang durch ein Passwort gesichert sind.[63] Zu beachten ist auch, dass bereits die Beschaffung der Zugangsdaten und Passwörter als vorbereitende Tat nach § 202c StGB strafbar ist.

Da das Lesen von privaten Nachrichten zudem eine Persönlichkeitsverletzung (insbesondere im Rahmen des Rechts auf informationelle Selbstbestimmung) darstellen kann, drohen gegebenenfalls auch Schadensersatzansprüche des Betroffenen aus § 823 BGB.

3.3.1.4 Vorsorgevollmacht: datenschutzrechtliche Betrachtung

Datenschutzrechtliche Bedenken gegen ein Einsichtsrecht des Bevollmächtigten ergeben sich jedenfalls dann nicht, wenn die Post- bzw. Fernmeldekontrolle unmissverständlich bzw. ausdrücklich in der Bevollmächtigung Niederschlag gefunden hat. Eine darauf basierende Datenverarbeitung wäre aufgrund einer solchen Einwilligung nach Art. 6 I 1 lit. a bzw. Art. 9 II lit. a DSGVO gerechtfertigt. Voraussetzung für die Wirksamkeit der Einwilligung ist, dass der Bevollmächtigende die Einwilligung in informierter Weise abgibt, d. h. er muss über das Ausmaß des Einsichtsrechts im Bilde sein, was aber bei einer eindeutigen Formulierung in der Vorsorgevollmacht in der Regel der Fall sein dürfte.

Liegt keine unmissverständliche Regelung der Fernmeldekontrolle in der Vorsorgevollmacht vor und hat der Bevollmächtigende sein Einverständnis über die Fernmeldekontrolle auch nicht in einer sonstigen Handlung kundgetan, kann nicht vom Vorliegen einer datenschutzrechtlichen Einwilligung ausgegangen werden, da nach Art. 4 Nr. 11 DSGVO die Willensbekundung unmissverständlich sowie durch Erklärung oder eine sonstige eindeutige bestätigende Handlung erfolgen muss. Zwar kommt auch eine konkludente Einwilligung in Betracht,[64] doch es ist fraglich, ob eine solche bei einer Erteilung einer Generalvollmacht vorliegt. Dagegen spricht, dass nach Art. 6 I 1 lit. a DSGVO der Zweck bzw. die Zwecke der Datenverarbeitung bestimmt sein müssen. Aus Erwägungsgrund 33 DSGVO lässt sich der Umkehrschluss ziehen, dass die Zwecksetzung eher eng sein muss.[65] Ist aus der Vorsorge- bzw. Generalvollmacht der Zweck der Fernmeldekontrolle für den Bevollmächtigenden nicht offenkundig ersichtlich, kann die Vorsorge- bzw. Generalvollmacht daher auch nicht als konkludente

[62] *Eisele*, in: Schönke/Schröder (Hrsg.), StGB Kommentar, § 202 Rn. 4.
[63] *Eisele*, in: Schönke/Schröder (Hrsg.), StGB Kommentar, § 202a Rn. 6.
[64] Vgl. BeckOK DatenschutzR/Albers/Veit, Art. 6 Rn. 24.
[65] *Schantz* in: Simits/Hornung/Spiecker (Hrsg.), DSGVO, Art. 6 Rn. 9.

Einwilligung in die Fernmeldekontrolle angesehen werden. Soll die Vollmacht also etwaige Datenverarbeitungen durch den Bevollmächtigten umfassen, sollte sie hinreichend bestimmt formuliert werden, d. h. es sollten die konkreten Zwecke benannt werden, zu welchen Daten verarbeitet werden können (wie etwa Gesundheitssorge, Vermögenssorge, usw.).

Soll die Fernmeldekontrolle die Kommunikation umfassen, welche (auch) sensitive Daten im Sinne des Art. 9 I DSGVO des Bevollmächtigenden beinhaltet, so ist sogar eine ausdrückliche Einwilligung erforderlich gemäß Art. 9 I lit. a DSGVO. Eine konkludente Einwilligung scheidet für diese Fälle damit von vornherein aus.

Als weiterer Rechtfertigungsgrund kommt Art. 6 I 1 lit. b DSGVO in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Liegt der Vorsorge- bzw. Generalvollmacht im Innenverhältnis ein Vertrag (z. B. Auftrag, § 662 BGB) zugrunde, könnten die vom Bevollmächtigten zur Erfüllung seiner vertraglichen Pflichten erforderlichen Verarbeitungen nach dieser Vorschrift gerechtfertigt sein.[66]

Außerdem kommt als Rechtfertigungsgrund darüber hinaus noch die Interessenabwägung nach Art. 6 I 1 lit. f DSGVO in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Zu den berechtigten Interessen im Sinne der Vorschrift zählen neben den rechtlichen Interessen auch tatsächliche, wirtschaftliche oder ideelle Interessen.[67] Das Interesse der Bevollmächtigten, zum Wohle des Bevollmächtigenden dessen digitale Kommunikation zu kontrollieren, kann daher im Rahmen der Abwägung angesetzt werden. Auf der anderen Seite liegt in einer solchen Kontrolle ein nicht unerheblicher Eingriff in das Persönlichkeitsrecht bzw. das Recht auf informationelle Selbstbestimmung des Bevollmächtigenden vor. Eine Rechtfertigung erschwerend kommt hinzu, dass – anders als bei einer gerichtlich angeordneten Betreuung – der Bevollmächtigte keiner gerichtlichen Kontrolle unterliegt. Aus diesen Gründen dürfte eine Rechtfertigung über Art. 6 I 1 lit. f DSGVO wohl regelmäßig nicht in Betracht kommen. Jedenfalls stellt sie für die vorliegende Fallkonstellation keine ausreichend rechtssichere Legitimation zur Datenverarbeitung dar.

Handelt es sich um besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, kommt neben der bereits erwähnten Einwilligung nach Art. 9 II lit. a DSGVO eine Rechtfertigung nach Art. 9 II lit. c und f DSGVO in Betracht. Insoweit kann auf die obigen Ausführungen zur Betreuung verwiesen werden.

In Bezug auf die datenschutzrechtlichen Belange von Kommunikationspartnern des Betreuten können die obigen Ausführungen hinsichtlich der datenschutzrechtlichen Rechtfertigung eines Zugangs durch die Erben auf Online-Accounts des Erblassers auf die vorliegende Konstellation übertragen werden.[68] Insoweit kann beispielsweise in Fällen, in denen es sich um eine Einsicht in Kommunikationsinhalte

[66] So auch *Buchner*, FamRZ 2019, 635 (670).
[67] *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DSGVO, Art. 6 Rn. 146.
[68] Vgl. *Buchner*, FamRZ 2019, 665 (670).

handelt, die über soziale Medien verschickt wurden, von einer Rechtfertigung über Art. 6 I 1 lit. f DSGVO ausgegangen werden.[69]

3.3.1.5 Pflicht des Dienstanbieters zur Zugangsgewährung

Ein Betreuer ist nach wohl einhelliger Ansicht im Rahmen der analogen Postkontrolle auch gegenüber der Post zum Empfang und zum Herausgabeverlangen der an die betroffene Person adressierten Post berechtigt.[70] Zur Wahrnehmung seiner Aufgaben muss dem Betreuer daher auch gegenüber einem Anbieter digitaler Dienste ein entsprechender Anspruch zustehen. Auf die digitalen Angelegenheiten übertragen würde dies bedeuten, dass ein Dienstanbieter dem Betreuer auf dessen Verlangen hin und nach ordnungsgemäßem Nachweis seiner Berechtigung auch dann Zugang zu Accounts der fürsorgebedürftigen Person verschaffen muss, wenn diese selbst das Passwort nicht herausgeben kann oder will.

Zwar kommen dem Vorsorgebevollmächtigten keine amtsähnlichen Befugnisse wie dem Betreuer als gesetzlichem Vertreter zu. Ist aber eine ordnungsgemäße Bevollmächtigung erfolgt und wurde der Bevollmächtigte privatautonom zur Wahrnehmung dieser Aufgaben bestimmt, so ist ein Dienstanbieter verpflichtet, auch dem Vorsorgebevollmächtigten Zugang zu den Accounts des Vollmachtgebers zu gewähren, soweit sich der Bevollmächtigte ausreichend legitimieren kann. Auch unter diesem Gesichtspunkt ist eine ausdrückliche Bevollmächtigung des Vertreters zur eigenständigen Fernmeldekontrolle zu empfehlen.

Eine unberechtigte Weigerung stellt eine objektive Pflichtverletzung des Dienstanbieters gegenüber der fürsorgebedürftigen Person als Vertragspartner dar und kann bei Vorliegen der weiteren Voraussetzungen, insbesondere bei Entstehung eines Schadens, zu einem Schadensersatzanspruch aus § 280 I BGB führen.

3.3.2 Aktive Nutzung durch den Vertreter

Im Erbfall wird angenommen, dass durch eine aktive Weiternutzung von Accounts des Erblassers ein neues Vertragsverhältnis zwischen Dienstanbieter und Erben entsteht. Dies ist möglich, da der verstorbene Erblasser aus dem Vertragsverhältnis ausscheidet und mit dem oder den Erben ein neuer Vertragspartner zur Verfügung steht.

Diese Argumentation lässt sich jedoch auf die Situation der (gesetzlichen oder gewillkürten) Stellvertretung durch Betreuer oder Vorsorgebevollmächtigte nicht unbesehen übertragen, da der ursprüngliche Nutzer noch als Vertragspartner zur Verfügung steht. Zudem ist zu berücksichtigen, dass der Vertreter den Account bzw. digitalen Dienst nicht als seinen eigenen nutzen will, sondern eine Nutzung nur für und im Interesse der betroffenen Person erfolgen soll. Sowohl ein Betreuer als auch ein Vorsorgebevollmächtigter tritt als Stellvertreter neben den Nutzer.

[69] Vgl. auch die Ausführungen unten zum aktiven Nutzungsrecht.
[70] *Müller-Engels*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 1896 Rn. 55; DNotI-Report 2013, S. 148 (149).

Insoweit ist zu untersuchen, ob der Vertreter als Treuhänder bei entsprechender Ermächtigung nicht nur bereits vorhandene Nachrichten lesen und Inhalte einsehen darf, sondern auch selbst Nachrichten direkt vom Account des vertretenen Nutzers verschicken oder Inhalte teilen darf.

3.3.2.1 Betreuung: Familienrechtliche Betrachtung

Im Rahmen seines Aufgabenkreises ist der Betreuer in gerichtlichen und außergerichtlichen Angelegenheiten der gesetzliche Vertreter der betroffenen Person, § 1902 BGB, und somit auch hinsichtlich ihrer digitalen Angelegenheiten. Zu untersuchen ist nun, ob dies auch die digitale Kommunikation der betroffenen Person in dem Sinne umfasst, als der Betreuer befugt ist, die Online-Vertragsbeziehungen und die damit zusammenhängende Korrespondenz des Fürsorgebedürftigen unmittelbar von seinem Account für diesen weiterzuführen.

Dem könnte entgegenstehen, dass die aktive Nutzung des Kontos als allein auf den Nutzer bezogenes Recht sein höchstpersönliches Recht ist. Im Rahmen des Erbfalls wird aufgrund dessen die Vererbbarkeit des aktiven Nutzungsrechts verneint. Auch im Rahmen der Betreuung gilt, dass höchstpersönliche Rechte der fürsorgebedürftigen Person nicht durch den Betreuer wahrgenommen werden[71] und insbesondere nicht unter einen Einwilligungsvorbehalt gestellt werden können, vgl. § 1903 II BGB.

Fraglich ist daher, ob es sich bei der aktiven Nutzung auch um ein solches höchstpersönliches Recht des Nutzers handelt, das nicht durch den Betreuer als Stellvertreter wahrgenommen werden darf.

Jedenfalls handelt es sich hierbei um keinen Fall gesetzlich ausdrücklich angeordneter Höchstpersönlichkeit (wie beispielsweise bei Eheschließung, § 1311 BGB, oder testamentarischen Verfügungen, §§ 2064, 2274 BGB), für die eine Vertretung generell nicht möglich ist.[72] Allerdings könnte die Stellvertretung aufgrund der höchstpersönlichen Natur des Rechts auf Nutzung von Accounts und Profilen ausgeschlossen sein.[73]

Möglicherweise hilft jedoch auch hier – wie im Rahmen der Beurteilung der Vererbbarkeit – der Vergleich mit dem Girovertrag. Im Erbfall tritt der Erbe durch die Weiternutzung eines Girovertrages selbst in den Vertrag ein und begründet eine eigene persönliche Rechtsbeziehung aus eigenem Recht und im eigenen Interesse mit der Bank. Die sich aus dem Vertragsverhältnis ergebenden Rechte und Pflichten sind dann nicht mehr vom Erblasser abgeleitet, sondern sind dem Erben persönlich zuzuordnen.[74] Wie in Kapitel 2.2 auf Seite 36 bereits ausführlich erläutert, überträgt die überwiegende Ansicht in der Literatur diese Grundsätze auf die Vererbbarkeit des digitalen Nachlasses. Angedeutet wird diese Beurteilung auch im Urteil des BGH zur Vererbbarkeit eines Facebook-Accounts.[75]

[71] *Müller-Engels*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 1902 Rn. 10 f.; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 220.

[72] Ausführlich dazu statt aller *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 25–46.

[73] Zu dieser Unterscheidung *Müller-Engels*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 1902 Rn. 10; *Bienwald*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1902 Rn. 53.

[74] Insofern die Argumentation des *BGH* zur Vererbbarkeit von Giroverträgen, siehe *BGH*, NJW 1996, 190 (191).

[75] BGH, NJW 2018, 3178 (3181).

Im Rahmen der Betreuung ist der Betreuer demgegenüber gemäß §§ 1812, 1813 I Nr. 3 BGB i. V. m. § 1908i I 1 BGB befugt, (genehmigungsfrei) Guthaben von Girokonten der betroffenen Person abzuheben und Überweisungen zu tätigen,[76] und (insoweit strittig, ob genehmigungsbedürftig oder nicht) die Kündigung zu erklären.[77] Nach zutreffendem Verständnis des § 1813 I Nr. 3 BGB ist auch die Überweisung vom Konto der betreuten Person genehmigungsfrei. Unter Berücksichtigung des damit verbundenen Aufwands sowie der Kosten und Risiken, ist der Betreuer nicht verpflichtet, zunächst das Geld vom Girokonto der betroffenen Person abzuheben, um es dann sofort von seinem eigenen Konto einem Gläubiger der betreuten Person zu überweisen bzw. auszuzahlen.[78] Insoweit entsteht hier nicht wie im Erbfall ein neues, eigenes Rechtsverhältnis zwischen Betreuer und Bank, sondern das Vertragsverhältnis zwischen Bank und Fürsorgebedürftigem bleibt bestehen, und der Betreuer nimmt als Stellvertreter und Treuhänder kraft gerichtlicher Anordnung[79] dessen Rechte und Pflichten wahr.

Dies lässt sich jedenfalls direkt auf die Befugnisse des Betreuers gegenüber reinen Online-Banken übertragen. Allein das tatsächliche Geschäftsmodell einer Bank kann an den Betreuerbefugnissen nichts ändern. Entsprechende Befugnisse hat der Betreuer auch bezüglich Transaktionen bei Online-Bezahldiensten.

Überträgt man diese Grundsätze auf die aktive Nutzung von Nutzerkonten der betroffenen Person, ist der Betreuer als Stellvertreter befugt, ihre Korrespondenz unmittelbar von ihrem Nutzerkonto für diese zu führen und damit Nachrichten direkt von diesem Account zu versenden. Der Betreuer nutzt das betreffende Nutzerkonto – genauso wie das Girokonto – nicht im eigenen Interesse, sondern als Stellvertreter der fürsorgebedürftigen Person in deren Interesse, § 1902 BGB. Dadurch soll keine eigene persönliche Rechtsbeziehung zwischen Betreuer und Bank bzw. Dienstanbieter entstehen. Vielmehr ist der Betreuer nur Treuhänder, der die Rechte und Pflichten sowie die Angelegenheiten des Nutzers für diesen fremdnützig wahrnimmt, soweit dies erforderlich ist, weil dieser sie nicht selbst besorgen kann. Im Innenverhältnis hat der Betreuer die Angelegenheiten der betroffenen Person so auszuüben, wie es deren Wohl entspricht, und ihre Wünsche zu berücksichtigen, § 1901 II, III BGB.[80] Es handelt sich insoweit um ein (gesetzliches) treuhänderisches Rechtsverhältnis.[81]

Der Betreuer ist dabei wie bei jedem treuhänderischen Handeln wesentlich an den (mutmaßlichen) Willen der betreuten Person als Treugeber gebunden[82] und somit nur die ausführende Hand, die der Selbstbestimmung der betroffenen Person zur Wirksamkeit verhelfen soll. Auch hier ist es nicht sachgerecht, wenn der Betreuer zunächst über das Nutzerkonto der betroffenen Person Einsicht nimmt und so von Nachrichten Kenntnis erlangt, um diese anschließend über sein eigenes Nutzerkonto

[76] *Kroll-Ludwigs*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1812 Rn. 13 ff., zur Überweisung insb. Rn. 16.
[77] *Kroll-Ludwigs*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1812 Rn. 20, § 1813 Rn. 2.
[78] *Kroll-Ludwigs*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1813 Rn. 13; *Veit*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 1813 Rn. 19; *Fröschle*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1813 Rn. 20.
[79] *Löhnig*, Treuhand, S. 158.
[80] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 15 f.
[81] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 1.
[82] *Löhnig*, Treuhand, S. 185.

(beispielsweise seinen E-Mail-Account) oder durch einen Brief – unter Erläuterung des Betreuungsverhältnisses sowie den Umständen seiner Kenntnisnahme von der Nachricht, auf die er sich bezieht, – beantworten zu müssen.

Hinsichtlich der Höchstpersönlichkeit ist zudem zu beachten, dass der Betreuer auch berechtigt ist, in seiner Stellvertreterfunktion analoge Briefe der betroffenen Person zu beantworten, auf persönliche Einladungen etc. zu reagieren, ohne dass diese Befugnis angezweifelt wird. Allein aufgrund der Tatsache, dass im Rahmen der digitalen Angelegenheiten das Übertragungsmedium ein anderes ist, kann die rechtliche Bewertung nicht wesentlich anders ausfallen.

Nicht notwendig erscheint auch, die aktive Nutzung von Nutzerkonten als eigene Aufgabe an den Betreuer zu übertragen. Vielmehr handelt es sich bei der aktiven Nutzung um eine notwendige Kompetenz zur Erfüllung des übertragenen Aufgabenkreises. Genauso wie der Betreuer auf analog übermittelte Briefe im Rahmen seines Aufgabenkreises antworten kann und können muss, steht ihm diese Befugnis hinsichtlich digital übermittelter Mitteilungen zu.

3.3.2.2 Betreuung: Datenschutzrechtliche Betrachtung

In Bezug auf das Verhältnis des Betreuers zum Betreuten ergeben sich aus datenschutzrechtlicher Sicht keine Unterschiede zu den Ausführungen, welche oben zu der Frage eines Einsichtsrechts des Betreuers getätigt wurden. Im Verhältnis zum Betreuten könnte eine aktive Nutzung zur Erfüllung der dem Betreuer übertragenen Pflichten daher nach Art. 6 I 1 lit. a bzw. lit. e DSGVO sowie nach Art. 9 II lit. a, lit. c und f DSGVO gerechtfertigt werden. Insoweit fehlt es allerdings auch hier an gefestigter Rechtsprechung.

In Bezug auf die datenschutzrechtlichen Belange von Kommunikationspartnern des Betreuten können die obigen Ausführungen hinsichtlich der datenschutzrechtlichen Rechtfertigung eines Zugangs durch die Erben auf Online-Accounts des Erblassers auf die vorliegende Konstellation übertragen werden.[83] In diesem Zusammenhang kann es insbesondere auf den Rechtfertigungsgrund des Art. 6 I 1 lit. f DSGVO und damit auf eine Interessenabwägung ankommen, wobei aufseiten des Betreuers (und des Betreuten) das Interesse an der Erfüllung der dem Betreuer übertragenen betreuungsrechtlichen Pflichten, aufseiten der Kommunikationspartner deren Grundrechte aus Art. 7 und 8 GRCh anzusetzen sind. Ferner ist zu berücksichtigen, dass es im berechtigten Interesse des Betreuten ist, dass Kommunikationsprozesse unter Einbindung einer helfenden Person weiterhin möglich sein sollen, sodass eine fortgesetzte Teilhabe am gesellschaftlichen Leben gewährleistet werden kann.[84] Auch sind die jeweiligen Umstände des Einzelfalles zu berücksichtigen, wie z. B., ob die Kommunikationspartner – wie bei der Nutzung von sozialen Plattformen – ihre Daten freiwillig und bewusst übermittelt haben und insoweit auch bewusst auf die Verfügungsbefugnis ihrer Nachrichten verzichten.[85]

[83] Vgl. *Buchner*, FamRZ 2019, 665 (670).
[84] *Buchner*, FamRZ 2019, 665 (671).
[85] Vgl. BGH, NJW 2018, 3178 (3187), *Buchner*, FamRZ 2019, 665 (671).

Eine pauschale Aussage, ob ein aktives Nutzungsrecht des Betreuers datenschutzrechtlich (un)zulässig ist, kann daher nicht getroffen werden. Obgleich in vielen Fällen von einer Rechtfertigung der Datenverarbeitung – sei es durch Einwilligung der betroffenen Person, sei es durch Vorliegen eines anderen Rechtfertigungsgrundes – ausgegangen werden kann, bleibt abzuwarten, wie sich die Rechtsprechung zu konkreten Einzelfällen entwickeln wird.

3.3.2.3 Vorsorgevollmacht: Familienrechtliche Betrachtung

Ein Vorsorgebevollmächtigter wird in dem Umfang als gewillkürter Stellvertreter tätig, in dem er privatautonom durch den Vollmachtgeber ermächtigt wurde.

Zu untersuchen ist nun, ob auch eine Bevollmächtigung zur Weiterführung der Online-Vertragsbeziehungen des Vollmachtgebers (uneingeschränkt) möglich ist.

Der Bevollmächtigung liegt als Schuldverhältnis in der Regel ein (entgeltlicher bzw. unentgeltlicher) Auftrag oder Geschäftsbesorgungsvertrag zugrunde, der die Rechtsbeziehung von Vollmachtgeber und Bevollmächtigtem im Innenverhältnis und damit auch die Rechte und Pflichten des Bevollmächtigten gegenüber dem Vollmachtgeber regelt. Etwaige Beschränkungen im Innenverhältnis berühren zwar für sich genommen nicht die Wirkung der Vollmacht im Außenverhältnis.[86] Allerdings ist der Vollmachtgeber frei, den Umfang der Vollmacht nach seinem Willen auch im Außenverhältnis zu beschränken oder als Generalvollmacht zu erteilen. Dabei kann der Umfang der Vollmacht nicht nur auf personenbezogene oder vermögensrechtliche Angelegenheiten beschränkt werden,[87] sondern beispielsweise das Einsichtsrecht erlaubt, die selbstständige Weiterführung der Online-Vertragsbeziehungen ohne Rücksprache mit dem Vollmachtgeber im Einzelfall zu untersagen.

Sind die selbstständige Weiterführung und damit die Durchführung der Korrespondenz aber von der Vollmacht umfasst, steht der Übertragung mittels Vollmacht auch hier nicht die Höchstpersönlichkeit dieser Rechte entgegen. Zwar kann die Wahrnehmung höchstpersönlicher Rechte des Vollmachtgebers auch durch Vorsorgevollmacht nicht privatautonom auf einen Stellvertreter übertragen werden.[88] Auch der Vorsorgebevollmächtigte will jedoch grundsätzlich Vertragsbeziehungen des Vollmachtgebers nicht im eigenen Willen und aus eigenem Interesse weiterführen, sondern auch er wird als Treuhänder für den Vollmachtgeber fremdnützig tätig.[89]

Insoweit kann auch hier die Stellvertretung im Rahmen von Giroverträgen zum Vergleich heranzogen werden: Ist von der Vorsorgevollmacht die Befugnis zur Führung von Bankgeschäften umfasst, so ist der Vorsorgebevollmächtigte befugt, diese als Stellvertreter des Vollmachtgebers zu führen. Erneut entsteht kein eigenes Rechtsverhältnis zwischen Bevollmächtigtem und Bank, sondern das Vertragsverhältnis zwischen Bank und dem nun durch einen Bevollmächtigten vertretenen Vollmachtgeber wird fortgeführt. Der Vorsorgebevollmächtigte ist auch befugt, – ebenso wie im Rahmen der

[86] *Kropp*, FPR 2012, S. 9 (10).
[87] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 77.
[88] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), Beck OGK BGB, § 1896 Rn. 256.
[89] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (16 f.).

Betreuung soeben beschrieben, ohne dass jedoch die Einschränkungen der §§ 1812 ff. BGB für den Vorsorgebevollmächtigten gelten – direkt vom Konto des Vollmachtgebers Geld abzuheben und Überweisungen zu tätigen.[90]

Übertragen auf die Fortführung von Online-Vertragsbeziehungen ist der Bevollmächtigte – unter der Prämisse, dass dies von seiner Vollmacht umfasst ist – befugt, unmittelbar die Accounts des Vollmachtgebers für Transaktionen (bei Online-Banken oder Online-Bezahlportalen) und Korrespondenz (insbesondere bei E-Mail- und Social-Media-Accounts) des Vollmachtgebers zu nutzen.

Dabei hat er sich als Treuhänder maßgeblich am Willen des Vollmachtgebers als Treugeber zu orientieren. Über diese allgemeine Bindung an den Willen des Vollmachtgebers hinaus ist es diesem zudem möglich, ein Handlungsermessen des Bevollmächtigten durch seine Vorgaben im Innenverhältnis einzuschränken und ihm Leitlinien an die Hand zu geben, wie sich der Treuhänder in gewissen Situationen zu verhalten hat.[91]

Ist der Vorsorgebevollmächtigte nach der Vollmachtsurkunde allgemein ermächtigt, die persönlichen oder vermögensrechtlichen Angelegenheiten zu besorgen, ist davon grundsätzlich auch die Befugnis zur Weiterführung der Online-Vertragsbeziehungen und Weiternutzung der Accounts des Vollmachtgebers umfasst, da dies in der Regel zur ordnungsgemäßen Ausübung der Vollmacht notwendig ist. Die Weiternutzung ist dem Bevollmächtigten damit nur dann nicht erlaubt, wenn sich dies ausdrücklich aus der Vollmacht ergibt.

3.3.2.4 Vorsorgevollmacht: Datenschutzrechtliche Betrachtung

In Bezug auf das Verhältnis des Bevollmächtigten zum Bevollmächtigenden ergeben sich aus datenschutzrechtlicher Sicht keine Unterschiede zu den Ausführungen, welche oben zu der Frage eines Einsichtsrechts des Bevollmächtigten getätigt wurden. Eine aktive Nutzung zur Erfüllung der dem Bevollmächtigten übertragenen Pflichten bzw. Befugnisse könnte daher nach Art. 6 I 1 lit. a bzw. lit. b DSGVO sowie nach Art. 9 II lit. a, lit. c und f DSGVO gerechtfertigt werden. Insoweit fehlt es allerdings auch hier an gefestigter Rechtsprechung.

In Bezug auf die datenschutzrechtlichen Belange von Kommunikationspartnern des Bevollmächtigenden können die obigen Ausführungen hinsichtlich der datenschutzrechtlichen Rechtfertigung eines Zugangs durch die Erben auf Online-Accounts des Erblassers auf die vorliegende Konstellation übertragen werden.[92] Hierzu gelten die obigen Ausführungen sinngemäß zu einem aktiven Nutzungsrecht des Betreuers im Betreuungsverhältnis. Das bedeutet, dass die Rechtfertigung insbesondere von einer Interessenabwägung nach Art. 6 I 1 lit. f DSGVO abhängen kann, sofern keine Einwilligung vorliegt.

[90] LG Detmold, ZEV 2015, 353 (354).
[91] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (18).
[92] Vgl. *Buchner*, FamRZ 2019, 665 (670).

Eine pauschale Aussage, ob ein aktives Nutzungsrecht des Bevollmächtigten datenschutzrechtlich (un)zulässig ist, kann daher nicht getroffen werden. Obgleich in vielen Fällen von einer Rechtfertigung der Datenverarbeitung – sei es durch Einwilligung der betroffenen Person, sei es durch Vorliegen eines anderen Rechtfertigungsgrundes – ausgegangen werden kann, bleibt abzuwarten, wie sich die Rechtsprechung zu konkreten Einzelfällen entwickeln wird.

3.3.2.5 Folgen der Nutzung durch den Stellvertreter

Nutzt der Stellvertreter nun den Account der betroffenen Person, erscheint es hinsichtlich des notwendigen Schutzes des Rechtsverkehrs einerseits als problematisch, wenn Betroffener und Vertreter über denselben Account Erklärungen abgeben könnten, ohne dass für den Empfänger bzw. den Rechtsverkehr allgemein erkennbar ist, wer der Verfasser der Nachricht ist. Andererseits kann es geschehen, dass der für den Online-Vertragspartner nicht erkennbar geschäftsunfähige Betroffene (unwirksame) Verträge abschließt, deren Durchsetzung anschließend abgewehrt werden muss.

Doppelzuständigkeit

Ist die fürsorgebedürftige Person noch geschäftsfähig, handelt es sich jedoch jedenfalls hinsichtlich der Wirksamkeit abgegebener Erklärungen um ein allgemeines Problem der Doppelzuständigkeit. Der Betreuer tritt zwar im Rahmen seines Aufgabenkreises im Außenverhältnis als der gesetzliche Vertreter der betroffenen Person auf (§ 1902 BGB). Trotzdem bleibt die fürsorgebedürftige Person grundsätzlich selbst geschäfts- und handlungsfähig, soweit nicht ein Einwilligungsvorbehalt nach § 1903 BGB angeordnet wurde, oder die Voraussetzungen des § 104 Nr. 2 BGB vorliegen.[93] Auch durch den Eintritt der Wirksamkeit einer Vorsorgevollmacht verliert die fürsorgebedürftige Person nicht automatisch ihre Handlungsfähigkeit, solange sie geschäftsfähig ist.[94]
Im Übrigen treten der Betreuer, soweit sein Aufgabenkreis reicht, und der Vorsorgebevollmächtigte, soweit seine Vollmacht, neben den Betroffenen im Rechtsverkehr auf,[95] sodass zwei Personen wirksam mit Rechtswirkung für und gegen den Nutzer im Rechtsverkehr auftreten können. Daher wird die betroffene Person sowohl aus den von ihr selbst als auch aus den durch den Stellvertreter für sie vorgenommenen Rechtsgeschäften berechtigt und verpflichtet. Steht ein vom Betroffenen abgeschlossenes Rechtsgeschäft einmal in Widerspruch zu einem vom Betreuer abgeschlossenen Rechtsgeschäft, gilt im Fall der Betreuung der Prioritätsgrundsatz,[96] der grundsätzlich auch auf die digitalen Angelegenheiten übertragen werden kann.

Erkennbarkeit im Rechtsverkehr

Problematisch erscheint es allerdings, dass im digitalen Rechtsverkehr nicht ohne Weiteres erkennbar ist, von wem eine Nachricht stammt.

[93] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 7.
[94] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 223 ff.
[95] *Dethloff*, FamR, § 17 Rn. 3.
[96] *Dethloff*, FamR, § 17 Rn. 3, 35; *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1902 Rn. 22.

Erkennbar ist der Absender zunächst nur über die E-Mail-Adresse oder den Nutzernamen bei Kommunikationsplattformen mit Chat- oder Nachrichtenfunktion. Der Rechtsverkehr könnte insoweit schutzwürdig sein, als Nachrichten nicht von einer anderen als der vermuteten bzw. mit dem Account im Regelfall verknüpften Person stammen sollten, insbesondere weil eine Identitätskontrolle nicht ohne Weiteres möglich ist.
Dem lässt sich jedoch zunächst entgegenhalten, dass die Anonymität des digitalen Rechtsverkehrs immer die Gefahr birgt, dass nicht die gedachte oder vermutete Person der Absender einer Nachricht ist, womit ein verständiger Nutzer auch grundsätzlich rechnen muss. Auch zeigt wieder der Vergleich mit dem analogen Briefverkehr, dass auch bei einem maschinengeschriebenen Brief ohne (lesbare) Unterschrift nicht ohne Weiteres ersichtlich ist, wer diesen abgesandt hat. Trotzdem ist der Vertreter aber befugt, Briefe zur Erfüllung seines Aufgabenkreises zu versenden. Um Täuschungen oder Irrtümern hier vorzubeugen, hat der Vertreter einen Hinweis auf das Bestehen des Betreuungs- bzw. Bevollmächtigungsverhältnisses zu geben und die Vertretungssituation kenntlich zu machen.

Diese Pflicht trifft den Stellvertreter auch im Rahmen der Nutzung von digitalen Kommunikationskanälen der fürsorgebedürftigen Person. Bezogen auf den E-Mail-Verkehr kann insoweit entweder eine Erklärung über die Betreuungs-/Bevollmächtigungssituation jeder individuellen E-Mail beigefügt werden oder eine generelle Erklärung gegenüber dem jeweiligen Kommunikationspartner abgegeben werden, dass E-Mails von der E-Mail-Adresse des Betroffenen in Zukunft durch den Vertreter verfasst werden. Insbesondere, wenn die betroffene Person aber noch selbst Zugriff auf das E-Mail-Konto hat und Nachrichten von diesem versendet, ist die Darlegung der Stellvertretung in der jeweiligen E-Mail zu empfehlen.

Dies lässt sich auf die Nutzung eines Social-Media-Accounts übertragen. Insoweit kann entweder auf der Profilseite[97] ein genereller Vertretungshinweis oder im Rahmen der entsprechenden individuellen Kommunikation eine Vertretererklärung abgegeben werden.

Beachtung datenschutzrechtlicher Vorgaben

Wenn die aktive Nutzung des Vertreters als datenschutzrechtlich relevante Datenverarbeitung anzusehen ist (was je nach Einzelfall variieren kann),[98] unterliegt der Vertreter den Pflichten, die sich aus der DSGVO ergeben. Insoweit gelten also die allgemeinen datenschutzrechtlichen Vorschriften.[99]

3.3.3 Kündigungsrecht

Richtigerweise soll allein die Anordnung nach § 1896 IV BGB nicht zur Kündigung eines Vertrages mit einem Telekommunikations- bzw. Dienstanbieter berechtigen.[100] Dies gilt schon deshalb, weil es sich

[97] Bei Facebook z. B. in der Info auf der Pinnwand, bei Instagram in der bio.

[98] Zu verneinen wäre dies z. B. bei einem nahen Verwandten als Vorsorgebevollmächtigten, der die Nutzung des für private Zwecke geführten Social-Media-Accounts als Gefälligkeitsdienst gegenüber dem Bevollmächtigenden erbringt.

[99] Beispielsweise muss der Vertreter die betroffenen Personen nach Art. 13 DSGVO informieren, er ist Anspruchsgegner bei der Ausübung von Betroffenenrechten, er muss geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO treffen, etc.

[100] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 287.

bei der Übertragung der Fernmeldekontrolle nicht um einen eigenen Aufgabenkreis handelt, sondern dies stets nur Annexkompetenz eines anderen Aufgabenkreises ist.

Die Kündigung eines Vertragsverhältnisses kann aber dann vom Aufgabenkreis der Vermögenssorge umfasst sein, wenn der Betreuer dies zum Wohle der fürsorgebedürftigen Person für erforderlich hält. Im Rahmen der Vermögenssicherungs- und -erhaltungspflicht kann die Kündigung angezeigt sein, wenn die Vertragsdurchführung mit Kosten verbunden ist, die entweder die Mittel des Betroffenen übersteigen, oder wenn er ohnehin nicht mehr in der Lage ist, den Dienst zu nutzen. Dies kann beispielsweise im Rahmen von Vertragsbeziehungen zu kostenpflichtigen Online-Spielen oder Streamingportalen mit monatlich anfallenden Kosten der Fall sein.

Schwieriger ist dies im Rahmen der Personensorge einzuordnen. So könnte der Betreuer oder Vorsorgebevollmächtigte einen Social-Media-Account löschen wollen, um so von der betroffenen Person über diesen Account unterhaltene psychisch belastende Kontakte effektiv zu unterbinden. Dies erscheint einerseits problematisch, weil so im Zweifel[101] die mit dem Account verknüpften Daten verloren gehen, beispielsweise alle gesendeten Nachrichten, Bilder, Posts, Verlinkungen etc., die mit *allen* Kommunikationspartnern des Betroffenen geteilt wurden und möglicherweise mit dem belastenden Kontakt überhaupt keine Verbindung haben. Dies ist mit dem Selbstbestimmungsrecht der fürsorgebedürftigen Person wohl kaum vereinbar. Hinsichtlich dieser Daten steht dem Vertreter wohl auch keine Verfügungsbefugnis zu. Zudem ist die gänzliche Löschung in den meisten Fällen nicht erforderlich und verhältnismäßig, weil der oder die belastenden Kontakte ausreichend im Rahmen der Kontrollbefugnisse nach § 1896 IV BGB eingedämmt werden können. Insofern ist ein Kündigungsrecht wohl nur in sehr engen Ausnahmefällen von der Vertretungsbefugnis umfasst.

Etwas anderes kann nur gelten, wenn der Betroffene den Vorsorgebevollmächtigten in einer Vorsorgevollmacht privatautonom ermächtigt hat, auch Nutzungsverträge mit Personenbezug zu kündigen und somit die Löschung der Accounts herbeizuführen.

Fällt die konkrete Nutzung von Online-Nutzerkonten in den Anwendungsbereich der DSGVO, können im Einzelfall Betroffenenrechte Dritter einer Kündigung (und damit einer Löschung der sie betreffenden Daten) entgegen stehen. Insoweit wird auf die Ausführungen zum Kündigungsrecht durch die Erben verwiesen.

3.4 Zusammenfassung

Auch im Rahmen seiner digitalen Angelegenheiten kann ein Nutzer von Online-Diensten sich somit im Fall seiner Handlungsunfähigkeit eines Stellvertreters bedienen. Dabei steht ihm die Möglichkeit offen, selbst privatautonom einer Person eine Vorsorgevollmacht zu erteilen. Ist dies nicht erfolgt,

[101] Dies gilt beispielsweise nicht uneingeschränkt bei Facebook. Dort kann der Nutzer auswählen, ob ein Konto und die damit verbundenen Daten vollständig gelöscht oder nur „deaktiviert“ werden sollen, sodass die Profilseite für Dritte nicht mehr sichtbar ist. Meldet sich der Nutzer nach der Deaktivierung jedoch erneut mit seinen Zugangsdaten an, wird das Profil unverändert wieder sichtbar und kann weiter genutzt werden.

kann auch ein gerichtlich bestellter Betreuer im Umfang seines Aufgabenkreises für die betroffene Person tätig werden.

Der (gesetzliche bzw. gewillkürte) Stellvertreter kann dabei die relevanten Handlungen für den Vertretenen vornehmen. Der Stellvertreter ist befugt, auf lokalen Speichermedien des Vertretenen oder auf Servern von Dienstanbietern gespeicherte Daten einzusehen sowie Online-Nutzerkonten des Vertretenen aktiv zu nutzen oder zu kündigen, soweit dies einerseits für die Stellvertretung erforderlich ist und soweit andererseits seine Ermächtigung reicht. Dies gilt – trotz unterschiedlicher rechtlicher Begründung – sowohl für den Betreuer als auch für den Vorsorgebevollmächtigten.

Die hier beschriebene Tätigkeit des Stellvertreters kann im Einzelfall datenschutzrechtliche Pflichten auslösen. Insoweit gelten die allgemeinen datenschutzrechtlichen Bestimmungen der DSGVO. Hierbei kann in vielen Fällen insoweit von einer Rechtmäßigkeit der Datenverarbeitung durch den Stellvertreter ausgegangen werden, allerdings fehlt es bislang noch an ausreichend gefestigter Rechtsprechung, um rechtssichere, allgemeingültige Aussagen treffen zu können.

Rechte und Pflichten eines Betreuers

Wird ein Nutzer digitaler Dienste (im Folgenden betroffene Person) alters- oder krankheitsbedingt fürsorgebedürftig und kann er seine Angelegenheiten nicht mehr selbst besorgen, kann durch ein Gericht ein Betreuer bestellt werden. Dies kann auch zu dem Zweck der Erledigung sogenannter digitaler Angelegenheiten erfolgen. Die digitalen Angelegenheiten können dabei all jenes umfassen, was bereits unter dem Begriff des digitalen Nachlasses beschrieben wurde. Die Betreuung kann in diesem Fall angeordnet werden, wenn die betroffene Person digitale Dienste und Angebote bisher in ihrem Alltag genutzt hat, nun aber nicht mehr in der Lage ist, sich selbst um diese zu kümmern und diese zu verwalten. Dabei wird die Betreuung selten für alle digitalen Dienste zugleich angeordnet, sondern nur für solche, bei denen eine Betreuung durch ein Gericht für notwendig erachtet wird.

Im Rahmen der Aufgaben, die dem Betreuer gerichtlich übertragen wurden, und soweit dies zur Erfüllung der Aufgaben erforderlich ist, darf der Betreuer grundsätzlich die digital geführte Kommunikation der betroffenen Person einsehen. Dies geschieht in der Regel dadurch, dass die betroffene Person entweder die Nachrichten selbst öffnet und diese an den Betreuer weiterleitet, oder betroffene Person und Betreuer gemeinsam die Nachrichten sichten und lesen. Ohne die betroffene Person darf der Betreuer die digitale Post nur dann lesen, wenn die betroffene Person hierzu ausdrücklich ihre Einwilligung erteilt hat oder – falls sie zur Einwilligung nicht in der Lage ist oder diese verweigert – dies durch ein Gericht gesondert angeordnet wurde.

Der Betreuer darf jedoch nicht die gesamte digitale Post der betroffenen Person lesen, sondern nur diejenige, die für die ihm übertragenen Aufgaben relevant ist. Ist

der Betreuer beispielsweise nur bestellt, um Vermögensangelegenheiten der betroffenen Person zu besorgen, darf er keine Einsicht in ihre Social-Media-Accounts nehmen, über die nur persönliche Nachrichten versendet werden. Werden über einen E-Mail-Account – wie im Regelfall – auch vermögensrelevante Geschäfte abgewickelt, darf der Betreuer zwar grundsätzlich Einsicht in den Account nehmen, aber nur die Nachrichten lesen, die für seine Betreueraufgaben relevant sind. Persönliche Nachrichten darf der Betreuer nur lesen, wenn sein Aufgabenkreis die persönlichen Angelegenheiten umfasst und von einer Kommunikationsplattform für den Verbraucher belastende (gegebenenfalls sogar gesundheitsgefährdende) Kontakte ausgehen, die durch den Betreuer zum Schutz der betroffenen Person abgewehrt werden sollen. Insgesamt darf eine Betreuung nur angeordnet und der Betreuer tätig werden, wenn die betroffene Person – auch zu ihrem eigenen Schutz – für Rechtshandlungen gegenüber dritten Personen einen Stellvertreter benötigt. Keiner Betreuung bedürfen daher in der Regel z. B. private Blogs oder Online-Tagebücher.
Ist ein Online-Vertrag für die Betreuung relevant, ist der Betreuer auch befugt, die zugehörigen Accounts zur Erfüllung seiner Aufgaben aktiv zu nutzen. So ist der Betreuer ermächtigt, im Rahmen von Online-Bezahldiensten Zahlungen in Auftrag zu geben oder zu stornieren sowie Nachrichten direkt vom Account der betroffenen Person zu beantworten. In letzterem Fall muss der Betreuer allerdings kenntlich machen, dass die Nachricht nicht von der betroffenen Person, sondern ihrem Betreuer stammt. Im Einzelfall ist der Betreuer auch befugt, zum Schutz des Vermögens der betroffenen Person überflüssig gewordene Online-Verträge zu kündigen.
Es kann davon ausgegangen werden, dass die Datenverarbeitung, die mit der hier beschriebenen Tätigkeit des Betreuers einhergeht, aus datenschutzrechtlicher Sicht gerechtfertigt werden kann. Die allgemeinen Vorschriften der DSGVO sind zu beachten.

Rechte und Pflichten eines Vorsorgebevollmächtigten
Möchte ein Verbraucher verhindern, dass im Fall seiner Fürsorgebedürftigkeit eine Betreuung angeordnet wird, kann er – solange er noch handlungs- und geschäftsfähig ist – einer Person eine Vorsorgevollmacht erteilen. Ist der Verbraucher aufgrund seines Alters oder aus gesundheitlichen Gründen anschließend nicht mehr in der Lage, seine Angelegenheiten selbst zu besorgen, wird somit der Vorsorgebevollmächtigte in dem Umfang für ihn tätig, in dem er durch die Vollmacht des Verbrauchers selbst wirksam ermächtigt wurde. Der Vorsorgebevollmächtigte kann dabei

grundsätzlich in demselben Umfang wie ein Betreuer bevollmächtigt werden, um digitale Angelegenheiten zu besorgen (siehe zum Begriff die Infobox „Rechte und Pflichten eines Betreuers“).

Im Rahmen der ihm vom Vollmachtgeber erteilten Befugnisse darf der Bevollmächtigte in Nutzeraccounts des Vollmachtgebers Einsicht nehmen, diese aktiv nutzen und gegebenenfalls kündigen. Die Einsichtnahme kann auch hier gemeinsam mit dem Vollmachtgeber erfolgen. Soll der Bevollmächtigte aber die digitale Post des Vollmachtgebers eigenständig ohne den Vollmachtgeber einsehen können, muss er hierzu in der Vollmacht ausdrücklich ermächtigt werden. Ist dies geschehen, dürfen die Dienstanbieter dem Bevollmächtigten nicht den Zugang zu den Accounts des Vollmachtgebers verweigern.

Soweit dies von seiner Vollmacht umfasst ist, darf der Vorsorgebevollmächtigte beispielsweise auch direkt von Online-Bezahldienst-Konten des Vollmachtgebers Transaktionen durchführen und Nachrichten versenden. Im letzteren Fall hat der Bevollmächtigte aber auf die Vertretungssituation hinzuweisen.

All diese Befugnisse sind grundsätzlich von einer Generalvollmacht gedeckt. Lediglich das Recht zur selbstständigen Durchsicht der digitalen Post ist der Vollmacht gesondert hinzuzufügen. Zur Vorlage für eine Vorsorgevollmacht für die digitalen Angelegenheiten siehe unten.

Es kann davon ausgegangen werden, dass die Datenverarbeitung, die mit der hier beschriebenen Tätigkeit des Bevollmächtigten einhergeht, aus datenschutzrechtlicher Sicht gerechtfertigt werden kann. Die allgemeinen Vorschriften der DSGVO sind zu beachten.

Das Wichtigste in Kürze

» Auch in dem Fall, dass der Verbraucher sich aus gesundheitlichen Gründen nicht mehr selbst um seine Angelegenheiten kümmern kann, können seine auf eigenen oder fremden Servern gespeicherten Daten relevant werden.

» In diesem Fall kann dem Verbraucher durch ein Gericht ein Betreuer zur Seite gestellt werden. Ein Betreuer darf aber nicht bestellt werden, wenn der Verbraucher zu einer Zeit, als er noch gesund war, einer Vertrauensperson eine Vorsorgevollmacht erteilt hat.

» Dem Betreuer bzw. dem Vorsorgebevollmächtigten ist es nicht von vornherein untersagt, die gespeicherten Daten des Verbrauchers einzusehen, Nutzerkonten des Verbrauchers zu nutzen oder diese zu löschen. Dies gilt sowohl für die Daten, die der Verbraucher auf eigenen Servern gespeichert hat, als auch hinsichtlich der Daten, die auf Servern von Online-Dienstanbietern (z. B. Social-Media-Portale, Online-Bezahldienste) gespeichert sind.

» Der Betreuer darf dies aber nur, soweit die Aufgabe von seinem durch das Gericht bestimmten Aufgabenkreis umfasst ist und dem Wunsch und Willen des Betreuten entspricht.

» Der Vorsorgebevollmächtigte darf dies nur, soweit ihn der Verbraucher selbst durch die Vorsorgevollmacht ermächtigt hat.

4 Rechte an Daten

Dieses Kapitel untersucht,

- ob es erforderlich ist, ein absolutes Recht an Daten zu schaffen,
- wie ein absolutes Recht an Daten ausgestaltet sein könnte,
- welche Vorteile die Schaffung eines absoluten Rechts an Daten haben könnte,
- welche Ansprüche und Rechte Erben haben, um einen Schutz der Daten des Erblassers nach seinem Tod zu besorgen,
- wie sich die Unanwendbarkeit der DSGVO auf die Daten Verstorbener und auf das digitale Erbe auswirkt,
- auf welcher rechtlichen/gesetzlichen Basis Daten postmortal geschützt werden können,
- was unter einem postmortalen Datenschutz zu verstehen sein könnte,
- welche Möglichkeiten der Erblasser hat, das Verfahren mit seinen Daten nach seinem Tod vorsorglich zu regeln,

- ob gesetzgeberischer Handlungsbedarf besteht hinsichtlich etwaiger Informationspflichten von Online-Dienstanbietern,
- welche Vor- und Nachteile vertragliche und testamentarische Vorsorgemaßnahmen haben.

4.1 Absolute Rechte an Daten

In der Entscheidung des BGH, in welcher den Erben ein Anspruch auf Zugang zum Facebook-Account der Erblasserin zugesprochen wurde,[1] ging es noch um die Frage eines schuldrechtlichen Anspruchs, durch den die Erben einen Zugang zu Daten erhalten, welche die Erblasserin und ihre Kommunikationspartner betrafen. Dieses Kapitel widmet sich der Frage, ob und inwieweit Erben über einen schuldrechtlichen Anspruch auf Zugang zu Nutzerkonten hinaus möglicherweise ein absolut wirkendes Recht an Daten des Erblassers erwerben können.

Absolute Rechte beinhalten zwei grundlegende Funktionen. Der Inhaber eines absoluten Rechts kann einerseits Dritte von dem Recht bzw. der Nutzung des Rechts ausschließen (Ausschlussfunktion). Andererseits steht ihm die Befugnis zu, das Recht zu nutzen (Nutzungsfunktion). Absolute Rechte wirken gegenüber jedermann und sind nicht verjährbar, das bedeutet, sie bilden keinen gegen einen bestimmten Dritten gerichteten Anspruch.[2] Beispielsweise kann der Eigentümer einer Sache gemäß § 903 S. 1 BGB, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. Daneben sind auch Immaterialgüterrechte wie Firma, Marke, Design, Patent oder Urheberrecht als absolute Rechte zu klassifizieren. Beispielsweise hat der Urheber eines Werkes positive Handlungsrechte, wie Vervielfältigungs- und Veröffentlichungsrechte, aber auch negative Rechte, um andere von einer Einwirkung auf das Werk auszuschließen.

Bevor die Frage geklärt werden kann, ob und inwieweit Erben ein absolut wirkendes Recht an Daten erwerben können, bedarf es zunächst der Untersuchung, ob und inwieweit dem Erblasser absolute Rechte an den Daten zuzusprechen sind. Im Kern geht es hierbei zunächst um die Frage, ob absolute Rechte an Daten ent- oder bestehen können. Nach geltendem Recht existiert keine explizite Zuordnung von Daten zu Rechten, die als absolut zu qualifizieren sind.[3] Die Diskussion in der juristischen Literatur betrifft daher die Frage, ob es einer Erweiterung der bestehenden Rechtsordnung um absolute Rechtspositionen an Daten bedarf und wie solche absoluten Rechte an Daten ausgestaltet sein könnten bzw. sollten.

Die Frage nach einem absoluten Recht an Daten, oder – abstrakter ausgedrückt – nach einer Zuordnung von Daten, steht in direktem Zusammenhang zu der oft gestellten Frage, wem Daten „gehören“.[4] Der Vergleich zum zivilrechtlichen Eigentumsrecht liegt auf der Hand, zumal eine Zuordnung durch das Eigentumsrecht dergestalt stattfindet, dass der Inhaber des Eigentumsrechts mit Befugnissen in Bezug auf eine Sache im Sinne des § 90 BGB ausgestattet ist, die absolut, d. h. gegen jedermann, wirken. Nicht in direktem Zusammenhang wirkt dagegen der alternativ hierzu vorgebrachte Vorschlag in der Literatur, den Rechtsrahmen für einen Zugang zu Daten weiter auszugestalten. Es geht hierbei

[1] BGH, Urteil vom 12.7.2018 – III ZR 183/17 – NJW 2018, 3178.

[2] *Henrich*, in: BeckOK BGB, § 194 Rn. 16.

[3] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 35; *Markendorf*, ZD 2018, 409 (410); *Specht*, CR 2016, 228 (289); *Thalhofer*, GRUR-Prax 2017, 225 (226); *Zech*, CR 2016, 137 (146); im Bezug auf Eigentumsrechte: *Determann*, ZD 2018, 503 (505).

[4] Vgl. *Czychowski/Siesmayer*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, Rn. 15; vgl. *Grützmacher*, CR 2016, 485 (486); vgl. *Peschel/Rockstroh*, MMR 2014, 571 (571).

also nicht mehr um die Frage einer Inhaberschaft an einem Recht, das Daten per se innewohnen würde (d. h. welches Daten zugeordnet würde), sondern um die Frage, wie der Zugang zu Daten zu regeln ist, um den Interessen der am Markt beteiligten Akteure zu entsprechen und diese in einen Ausgleich zueinander zu bringen. Schwerpunkt dieser Studie ist die Frage nach einem absoluten Recht an Daten, also nach einer Zuordnung. Der Frage nach einem Zugang zu Daten wird daher nur insoweit nachgegangen, als sie für die Frage nach der Erforderlichkeit einer Zuordnung relevant ist.

Im Rahmen der Diskussion um ein absolutes Recht an Daten wird der Begriff Daten von der semantischen Information, d. h. dem Inhalt, abgegrenzt. Der hier verwendete Datenbegriff beinhaltet damit die Zeichenebene, d. h. die syntaktische Information. Das bedeutet, dass nicht die Frage nach einem Dateneigentum – beispielsweise allein an personenbezogenen Daten, also an den in den Daten verkörperten Informationen –, sondern an Daten im Allgemeinen, d. h. unabhängig von ihrem Inhalt, Gegenstand der juristischen Kontroverse ist. Teilweise wird der Ausgangspunkt der Betrachtung allerdings insoweit eingeschränkt, als personenbezogene Daten explizit von der Frage nach einem Dateneigentum ausgenommen werden, d. h. es findet insoweit eine inhaltliche Eingrenzung statt. Als Gründe hierfür werden beispielsweise vorgebracht, dass für diese mit dem Datenschutzrecht bereits ein gesonderter Rechtsrahmen bestehe,[5] und ein Regulierungsbedarf wegen der damit einhergehenden Begrenzungen der Vertragsfreiheit durch das Datenschutzrecht nicht gegeben sei.[6] Allerdings lässt sich die Frage nach einem Regelungsbedarf hinsichtlich absoluter Rechtspositionen an digitalen Daten nur angemessen untersuchen, wenn die gesamte Rechtsordnung in den Blick genommen wird, um so den bereits bestehenden Rechtsrahmen und den daraus folgenden Schutz in Bezug auf bestimmte Datenarten, wie etwa personenbezogene Daten, nicht außer Acht zu lassen.[7] Im Rahmen der hier vorgenommenen Untersuchung wird daher auch auf die Frage nach einem absoluten Recht an personenbezogenen Daten eingegangen. Dies ist insbesondere für Fragen der Vererbbarkeit von Daten zielführend, da Daten, an denen ein Interesse des Erblassers oder der Erben an der Vererbbarkeit besteht, oftmals als personenbezogene Daten zu qualifizieren sind, nämlich immer dann, wenn sie der Person des Erblassers zugeordnet werden können (beispielsweise durch den Vertragspartner des Erblassers). Die Frage nach einem absoluten Recht an Daten zielt also im Kontext des digitalen Nachlasses folglich auch auf die Vererbbarkeit personenbezogener Daten ab.

4.1.1 Mögliche Ausgestaltung eines absoluten Rechts an Daten

Im Folgenden werden zum besseren Verständnis überblicksartig wesentliche Aspekte eines neu zu schaffenden absoluten Rechts an Daten dargestellt:[8]

[5] *Czychowski/Siesmayer*, in: Kilian/Heussen, Computerrechts-Handbuch, Rn. 7; vgl. *Wiebe/Schur*, ZUM 2017, 461 (462).
[6] *Peitz/Schweitzer*, NJW 2018, 275 (278); vgl. *Ensthaler*, NJW 2016, 3473 (3473); vgl. *Thalhofer*, GRUR-Prax 2017, 225 (225).
[7] In diese Richtung geht auch die Untersuchung der *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 31 ff. und S. 45.
[8] Angelehnt an die Ausführungen der *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 38 ff.

4.1.1.1 Schutzumfang

Ein neu zu schaffendes absolutes Recht an Daten könnte – wie das Sacheigentum oder auch Immaterialgüterrechte – positive und negative Befugnisse für den Berechtigten beinhalten. Es könnte als Vollrecht oder auch nur hinsichtlich einzelner Befugnisse begründet werden. Zu den positiven Rechten könnten zählen:

- **Zugangsrecht**, d. h. der Berechtigte entscheidet darüber, ob er Daten geheim hält bzw. wem und auf welche Art und Weise er Zugang zu den Daten ermöglicht.
- **Herausgaberecht**, d. h. der Berechtigte kann die Herausgabe von Daten verlangen, die sich im Herrschaftsbereich von Dritten befinden. Eine Herausgabe könnte dann in der Übertragung (Kopie) und der Löschung der beim Dritten verbliebenen Daten ausgestaltet sein, oder aber der Dritte könnte weiterhin auf die Daten zugreifen (ähnlich wie beim Zugangsrecht nach § 25 UrhG, d. h. nur Herausgabe der Kopie).
- **Nutzungsrecht**, d. h. der Berechtigte kann darüber entscheiden, ob und inwieweit er Dritten die Nutzung der Daten ermöglicht. Infrage kommt eine exklusive oder eine nicht exklusive Nutzung (Teilhabe). In beiden Fällen kann die Nutzung zeitlich oder sachlich beschränkt eingeräumt werden (z. B. Nutzung nur für einen Monat, nur solange, wie ein Vertragsverhältnis besteht, usw.).
- **Verfügungsrecht**, d. h. der Berechtigte kann sein Recht an den Daten aufheben, verändern, oder auf Dritte übertragen.

Als negative Rechte sind Befugnisse zu verstehen, die mit dem positiven Recht einhergehen und eine Ausschlusswirkung beinhalten. Solche Rechte beinhalten z. B. das Recht, jede Störung durch Dritte, die der ungehinderten Ausübung der positiven Rechte entgegehensteht, abzuwehren.

4.1.1.2 Dogmatische Verortung

Neben der Schaffung einer neuen Kategorie kommt eine Anknüpfung an ein bestehendes absolutes Recht in Betracht. Es bieten sich hierfür das Sacheigentum sowie die bestehenden Immaterialgüterrechte wie das Patentrecht und das Urheberrecht an, ggf. ergänzt um Leistungsschutzrechte.[9]

Ein konkreter Vorschlag zur Verortung eines absoluten Rechts an Daten kann an dieser Stelle nicht getätigt werden, es sind aber gewisse Zweifel an einer Anlehnung an das Sacheigentum vorhanden: Ökonomisch beruht der Schutz des Sacheigentums auf der Idee der Einräumung einer exklusiven Nutzungsmöglichkeit. Dies folgt aus dem Umstand, dass körperliche Sachen regelmäßig exklusiv, d. h. von einer Person bzw. jedenfalls einer endlichen Zahl von Personen, nutzbar sind. Die Nutzung einer Sache schränkt ihre Nutzbarkeit durch andere ein und verringert so den Kreis der Nutzungsmöglichkeiten.[10] Daten sind jedoch technisch frei verfügbar und können beliebig oft kopiert werden, wobei

[9] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 39 ff.
[10] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 39 ff.

die Nutzung durch eine Person nicht die Nutzung anderer potenzieller Nutzer beeinträchtigt. Aus diesem Grund besteht auch keine Erforderlichkeit, die Nutzungsmöglichkeit durch die Schaffung eines absoluten Rechts – wie es beim Sacheigentum der Fall ist – zu monopolisieren und damit einem oder mehreren Rechtsinhabern exklusiv zuzuweisen.[11] Im Unterschied dazu gibt es gewisse Parallelen zwischen den spezifischen Eigenschaften von Daten und der Abgrenzung von eigenschöpferischem Werk einerseits und Werkstücken andererseits im Urheberrecht. Während die ursprünglichen Daten, sozusagen das Original, dem urheberrechtlich geschützten Werk gleichen, gleichen daraus gefertigte Kopien der Daten den Werkstücken im urheberrechtlichen Sinne. Durch die künstlich hergestellte Verknappung durch Schaffung eines Urheber-, Patent-, Marken- oder Designrechts wird ein Anreiz für wirtschaftliche Tätigkeit geschaffen.[12]

4.1.1.3 Besondere Ansätze

Die folgenden Punkte sind angelehnt an die Ausführungen der Arbeitsgruppe „Digitaler Neustart“.[13]

- **Recht an Daten als Registerrecht**: Nur registrierte Daten sollen geschützt werden. Mit einer Daten-Registrierung ginge eine gewisse Transparenz und Rechtssicherheit einher. Eine Ausgestaltung als Registerrecht würde allerdings am verfahrensmäßigen Aufwand scheitern, eine Registrierung aller personenbezogenen Daten, die tagtäglich im Internet verarbeitet werden, ist nahezu unmöglich. Hier bräuchte es eine technische Lösung, die das Verfahren praktikabel macht.
- **Datenschutz als Dateneigentums- oder Datenverwertungsrecht**: Zum Teil wird eine Weiterentwicklung des Datenschutzrechts diskutiert. Im Fokus stehen hierbei das Eigentum des Datenproduzenten an Daten sowie ein positives Nutzungs- und Verwertungsrecht, das einer Person zugewiesen werden kann.

4.1.2 Vergleichende Betrachtung

Einer Ausgestaltung der bestehenden Rechtsordnung dahingehend, dass eine Zuordnung von Daten im Sinne einer Dateninhaberschaft erreicht werden soll, bedarf es dann nicht, wenn die bestehenden Schutzregime einen ausreichenden Schutz von Daten gewährleisten.[14] Obwohl das Zivilrecht einen ausdrücklich geregelten Schutz von Daten gegenüber jedermann nicht vorsieht, sind Daten nicht schutzlos dem Zugriff Dritter ausgesetzt.[15] Auch aus verfassungsrechtlicher Sicht hängt die Frage nach einer Schaffung eines Eigentums oder eines anderen absoluten Rechts an Daten insbesondere

[11] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 40 ff.
[12] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 40 ff.
[13] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 41 ff.
[14] Vgl. *Czychowski/Siesmayer*, in: Kilian/Heussen, Computerrechts-Handbuch, Rn. 16; vgl. *Heymann*, CR 2016, 650 (650); vgl. *Markendorf*, ZD 2018, 409 (409); vgl. *Peschel/Rockstroh*, MMR 2014, 571 (574).
[15] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 35; vgl. auch *Markendorf*, ZD 2018, 409 (410).

davon ab, welcher Schutz Daten durch das geltende Recht zukommt.[16] Stellt sich heraus, dass ein ausreichender Schutz nicht vorhanden ist, können die bestehenden Regelungen möglicherweise als Ansätze zu einer Neugestaltung eines solchen absoluten Rechts dienen.[17]

Ob ein ausreichender Schutz von Daten besteht, kann unter Zuhilfenahme mehrerer Gesichtspunkte (wie etwa ökonomischer oder soziologischer Aspekte) untersucht werden. Da die Frage nach der Erforderlichkeit eines absoluten Rechts an Daten und damit auch nach einem ausreichenden Schutz von Daten in der vorliegenden Studie in die Thematik des digitalen Nachlasses eingebettet ist, wird ihr auch aus diesem Blickwinkel nachgegangen. Das bedeutet, dass auf Gesichtspunkte, die keine oder wenig Relevanz zu der Thematik des digitalen Nachlasses aufweisen, nicht eingegangen wird. Hierfür wird auf die einschlägige Literatur verwiesen.

Um mögliche Schutzlücken, welche sich aus dem Nicht-Vorhandensein eines absoluten Rechts an Daten ergeben, zu erfassen, können folgende Überlegungen zielführend sein:

- Welche Arten von Schutz würden durch ein absolutes Recht an Daten erreicht im Kontext des digitalen Nachlasses?
- Wie ist der Schutz ausgestaltet, der durch die bestehende Rechtsordnung für Daten im Kontext des digitalen Nachlasses erreicht wird?
- Welche Lücken im Kontext des digitalen Nachlasses ergeben sich aus einem Vergleich der bestehenden Rechtsordnung zu der Rechtsordnung, in deren ein etwaiges absolutes Rechts an Daten existiert?

4.1.2.1 Schutz gegen unberechtigten Zugriff und Recht zur wirtschaftlichen Verwertung als Funktionen eines absoluten Rechts an Daten

Ein absolutes Recht an Daten könnte mehrere Schutzrichtungen aufweisen. Ausgehend von den beiden grundlegenden Funktionen eines absoluten Rechts, nämlich der Ausschluss- und der Nutzungsfunktion, die der Berechtigte gegenüber jedermann geltend machen kann, würden in Bezug auf ein absolutes Recht an Daten folgende Schutzrichtungen entsprechen:[18]

- **Integritätsschutz von Daten**, d. h. Schutz vor Verlust oder Verfälschung der Daten,
- **Geheimnisschutz von Daten**, d. h. Schutz vor Zugriff durch Dritte,

[16] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 45, vgl. *Wiebe/Schur*, ZUM 2017, 461, die sich insbesondere mit dem Spannungsverhältnis zwischen Eigentum an Daten aus zivilrechtlicher und verfassungsrechtlicher Sicht auseinandersetzen.

[17] Vgl. *Czychowski/Siesmayer*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch Rn. 16; vgl. *Zech*, CR 2015, 137 (139 ff.).

[18] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 52 ff.; abweichende Kategorisierungen: vgl. *Becker*, FS Fezer, 2016, 815 (821ff.) mit ähnlichen Kriterien; vgl. *Grützmacher*, CR 2016, 485 (486) mit ähnlichen Kriterien; ebenfalls ähnlich vgl. *Zech*, CR 2015, 137 (140).

- **Schutz des Interesses an der Verwertung von Daten**, d. h. exklusive Zuordnung des Rechts auf wirtschaftliche Verwertung an den Berechtigten, welche einhergeht mit einem Schutz vor Verwertung durch Nichtberechtigte (z. B. durch Bereicherungs- und Schadensersatzansprüche).

Ein etwaiges absolutes Recht an Daten könnte so ausgestaltet werden, dass es nach dem Tod des Erblassers auf die Erben gemäß § 1922 BGB übergeht. Die genannten Schutzrichtungen könnten nach Eintritt des Erbfalls folglich den Erben zugute kommen. Wie oben bereits angesprochen, gibt es zahlreiche Überlegungen hinsichtlich der Ausgestaltung eines absoluten Rechts an Daten. Abschließende Schlussfolgerungen hinsichtlich des Bedarfs an Schutzrichtungen und Schutzintensität eines solchen absoluten Rechts können sinnvollerweise erst nach einer Untersuchung nach bestehenden Schutzlücken unter dem geltenden Recht getätigt werden.

4.1.2.2 Schutz gegen unberechtigten Zugriff und Recht zur wirtschaftlichen Verwertung in der bestehenden Rechtsordnung

Nachfolgend werden etwaige Ansprüche auf Herausgabe, d. h. der (Rück-)Übertragung und anschließender Löschung beim Anspruchsgegner, sowie Schadensersatz für den Fall des unberechtigten Datenzugriffs (d. h. der unberechtigten Datenverarbeitung) untersucht.

Vertragliche Ansprüche

Besteht zwischen dem Rechtsinhaber und dem infrage kommenden Anspruchsgegner ein vertragliches Verhältnis, welches den Zugriff bzw. die Verarbeitung von Daten (mit-)regelt, so ist in der Regel davon auszugehen, dass sich die Befugnis für den Datenzugriff bzw. die Datenverarbeitung aus dem Inhalt des Vertrages ergibt. Überschreitet eine Vertragspartei die sich aus dem Vertrag ergebende Befugnis zur Datenverarbeitung, können sich Schadensersatzansprüche aus dem Vertrag selbst sowie aus allgemeinem Leistungsstörungsrecht nach den §§ 280 ff. BGB ergeben.[19] Besteht keine vertragliche Beziehung zwischen dem Datenverarbeiter und dem Rechtsinhaber, so können möglicherweise die Grundsätze über den Vertrag mit Schutzwirkung zugunsten Dritter bzw. der Drittschadensliquidation greifen, was dann infrage kommt, wenn sich der Vertragspartner eines Dritten bedient, welcher ohne vom Rechtsinhaber erteilte Befugnis dessen Daten verarbeitet (z. B. Cloudbetreiber greift auf das Rechenzentrum eines Dritten zu, um seine vertraglichen Pflichten gegenüber dem Rechteinhaber zu erfüllen).[20]

Da mit dem Erbfall nach § 1922 BGB die Gesamtrechtsnachfolge eintritt, können vertragliche Ansprüche grundsätzlich vererbt und damit auch von den Erben geltend gemacht werden. Dies bedeutet, dass der Erbe in den Vertrag des Erblassers eintritt und damit die aus dem Vertrag ergebenden

[19] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 53.

[20] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 53; vgl. *Specht*, Konsequenz der Ökonomisierung informationeller Selbstbestimmung, S. 230 ff.

Rechte und Pflichten übernimmt. Das Prinzip der Gesamtrechtsnachfolge unterscheidet nicht zwischen analogem und digitalem Nachlass,[21] sodass der Umstand, dass der Vertrag den Zugang und ggf. die Nutzung von digitalen Daten beinhaltet, nicht schadet. Ausnahmen von diesem Grundsatz können dann vorliegen, wenn das Vertragsverhältnis derart auf die Person des Vertragspartners zugeschnitten ist, dass ein Eintritt durch den Erben nicht interessengerecht sein dürfte.

Gesetzliche Ansprüche

Eigentumsschutz des Speichermediums Sowohl das Eigentum als auch der Besitz an Sachen i. S. d. § 90 BGB und damit auch an Speichermedien sind umfassend geschützt, etwa nach den §§ 858 ff., 985 ff., 823 ff., 1004 und 812 ff. BGB. Da es anerkannt ist, dass der unberechtigte Zugriff auf gespeicherte Daten auch das durch § 903 BGB geschützte Eigentum an dem Speichermedium verletzt, kommt Daten auf Speichermedien einhergehend mit dem Eigentumsschutz ebenfalls ein Schutz zu.[22] Der Eigentumsschutz greift allerdings dann naturgemäß nicht, wenn das Speichermedium nicht im Eigentum des Rechtsinhabers der Daten ist.

Weitere absolute Rechte Neben vertraglichen und damit relativen Rechten kann Daten auch ein absolut, d. h. gegenüber Dritten wirkender Schutz zukommen. Daten sind unter strafrechtlichen, deliktsrechtlichen sowie insolvenzrechtlichen Gesichtspunkten vor Einwirkungen Dritter geschützt:

- §§ 202a ff., 303a StGB als Schutzgesetze i. S. d. § 823 II BGB

Die Straftatbestände der §§ 202a, 202b, 202c, 202d und 303a StGB schützen Daten unabhängig vom Speichermedium und ihrem Inhalt. Nach einhelliger Auffassung handelt es sich hierbei um Schutzgesetze i. S. d. § 823 II BGB.[23] Damit kann der unbefugte Zugriff auf Daten Ansprüche auf Schadensersatz und Unterlassen auslösen.

- Deliktsrechtlicher Schutz

Ein absolut wirkender deliktsrechtlicher Schutz an Daten kann sich aus § 826 BGB ergeben. Diese Vorschrift weist allerdings enge Tatbestandsvoraussetzungen auf, sodass wohl nur in Ausnahmefällen eine vorsätzliche sittenwidrige Schädigung gemäß § 826 BGB zu bejahen ist. Daneben kommt eine Haftung nach § 823 I BGB in Betracht. Außer dem bereits oben erwähnten Schutz des Eigentums und des berechtigten Besitzes am Speichermedium sind beispielsweise auch der eingerichtete und ausgeübte Geschäftsbetrieb und das allgemeine Persönlichkeitsrecht als sonstige Rechte im Sinne der Vorschrift geschützt. Als Ausprägungen des allgemeinen Persönlichkeitsrechts sind das postmortale Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung geschützt.[24]

In Bezug auf deliktsrechtliche Ansprüche ist zunächst zu unterscheiden, ob der jeweilige Anspruch zu Lebzeiten oder nach dem Tod des Erblassers begründet wurde. Ansprüche zu Lebzeiten gehen

[21] *Steiner/Holzer*, ZEV 2015, 262 (262).
[22] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 54.
[23] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 55 m. w. N.
[24] *Sprau*, in: Palandt BGB § 823 Rn. 85, 89f; vgl. OLG Oldenburg, Urteil vom 23.12.2014 – 13 U 66/14 – NJW-RR 2015, 724

grundsätzlich mit Eintritt des Erbfalls im Wege der Gesamtrechtsnachfolge gemäß § 1922 BGB auf den bzw. die Erben über. Ansprüche aus § 826 BGB bzw. aus § 823 I und § 823 II BGB i. V. m. einem Schutzgesetz können aber auch nach dem Tod des Erblassers entstehen, wobei die Erben, welche aufgrund der Gesamtrechtsnachfolge nunmehr Rechtsinhaber sind, originäre Anspruchsinhaber dieser deliktischen Ansprüche sind.

Eine Besonderheit stellt eine Verletzung des Allgemeinen Persönlichkeitsrechts dar. Wurde dieses zu Lebzeiten des Erblassers verletzt, gehen diesbezügliche Ansprüche mit Eintritt des Erbfalls auf die Erben über gemäß § 1922 BGB. Eine Verletzung nach dem Tod des Erblassers führt hingegen nicht zwangsläufig zu einer Anspruchsbegründung aus § 823 I BGB i. V. m. mit Art. 2 I, Art. 1 I GG, da das Allgemeine Persönlichkeitsrecht grundsätzlich nur lebende Personen schützt. Ein Schutz kann allerdings insoweit bestehen, als eine Verletzung des postmortalen Persönlichkeitsrechts vorliegt, welches auf Art. 1 I GG beruht. Diesbezüglich wird unterschieden zwischen nichtvermögenswerten und vermögenswerten Bestandteilen dieses Rechts: Da bei Verstorbenen eine handelnde Person nicht mehr existiert, ist der Schutz der Persönlichkeit bei ideellen Beeinträchtigungen eingeschränkt. Es besteht dann allenfalls ein Unterlassungs- oder Widerrufsanspruch, nicht aber ein Entschädigungsanspruch. Außerdem stehen die Ansprüche nicht den Erben, sondern den nächsten Angehörigen zu (welche auch Erben sein können).

Im Gegensatz dazu bestehen die vermögenswerten Bestandteile des Persönlichkeitsrechts fort und gehen auf die Erben über.[25] Eine Verletzung der vermögenswerten Bestandteile des Persönlichkeitsrechts kann damit zu einem Entschädigungsanspruch führen. Hierbei ist zu beachten, dass den Erben kein uneingeschränktes positives Benutzungsrecht kennzeichnender Persönlichkeitsmerkmale (wie z. B. des Namens oder des Bildnisses) zusteht, das auch gegen die ausdrücklichen oder mutmaßlichen Interessen des verstorbenen Trägers des Persönlichkeitsrechts eingesetzt werden könnte. Vielmehr ist eine Nutzung der nach dem Tode bestehenden Vermarktungsmöglichkeiten nur unter Berücksichtigung dieses Willens möglich.[26]

Fraglich ist, ob Daten bzw. ein Recht am eigenen Datenbestand als sonstiges Recht i. S. d. § 823 I BGB zu qualifizieren sind bzw. ist. Es ist anerkannt, dass nur absolute Rechte für eine Qualifizierung als sonstiges Recht i. S. d. § 823 I BGB in Betracht kommen, wobei es entscheidend auf die Ausschlussfunktion des jeweiligen Rechts ankommt, da die Nutzungsfunktion – welche auch schuldrechtlichen Ansprüchen zukommt – wenig Unterscheidungskraft hat.[27] Berücksichtigt werden muss außerdem die systematische Funktion des § 823 I BGB im Deliktsrecht, welche maßgeblich in der bewussten Nichtberücksichtigung reiner Vermögensschäden im Rahmen der Fahrlässigkeitshaftung besteht.[28]

Für die Anerkennung eines Rechts an Daten als sonstiges Recht im Sinne des § 823 I BGB spricht, dass ansonsten ein unterschiedliches Schutzniveau hinsichtlich solcher Daten bestünde, welche auf physischen Medien des Berechtigten gespeichert sind und damit einen über das Eigentums- bzw. Besitzrecht abgeleiteten Schutz nach § 823 I BGB genießen, und solchen Daten, welche in einer Cloud,

[25] *Sprau*, in: Palandt BGB § 823 Rn. 89 f.; BGH I ZR 49/97 – „Marlene Dietrich" – GRUR 2000, 709.
[26] BGH I ZR 49/97 – „Marlene Dietrich" – GRUR 2000, 709 (714).
[27] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 47; *Sprau*, in: Palandt BGB, § 823 Rn. 11.
[28] *Wagner*, in: MüKoBGB, § 823 Rn. 265.

d. h. auf fremden Servern gespeichert sind. Das Deliktsrecht würde seiner Aufgabe nicht gerecht, für neuartige Probleme, welche dem technischen Fortschritt und veränderten Bedürfnissen der Datennutzer geschuldet sind, passende Lösungen bereitzustellen.[29] Als Beleg für die Anerkennung des Dateneigentums als Rechtsgut wird außerdem der zum 01.08.2007 neu eingeführte Straftatbestand des § 303a StGB angeführt, welcher einen weiten Schutzbereich aufweise und damit im Gegensatz stehe zur Konstruktion eines indirekten Schutzes von Daten durch das Eigentum am Datenträger, welcher eben zu kurz greife. Da die strafbewehrten Verhaltenspflichten des § 303a StGB den Schutz eines Rechtsguts bezwecken, kann als Schutzgut nur ein Individualrecht an den eigenen Daten infrage kommen.[30]

Gegen eine Anerkennung eines Rechts an Daten als sonstiges Recht sprechen zunächst dogmatische Bedenken. Nach der Dogmatik der gefestigten Rechtsprechung reichen Ausschlussrechte auf vertraglicher Grundlage nicht aus, um eine gegenüber jedermann wirkende Rechtsposition zu begründen.[31] Eine rein faktische Ausschließlichkeit, wie sie etwa aufgrund rein technischer Gegebenheiten vorliegen kann, reicht für die Begründung eines absoluten Rechts nicht aus.[32] Darüber hinaus kommen rechtstechnische Bedenken hinzu.[33] Zum einen ließe sich der Schutzbereich an einem Recht am eigenen Datenbestand kaum definieren, zum anderen wäre es klärungsbedürftig, wem ein solches Recht zustehen sollte, was insbesondere bei automatisch generierten Daten problematisch sein dürfte. Außerdem geriete die Statuierung einer absolut wirkenden Rechtsposition an Daten insbesondere bei kollidierenden Rechten, die sich aus dem Inhalt der Daten ergeben, ins Wanken, wie beispielsweise dem allgemeinen Persönlichkeitsrecht bzw. dem Recht auf informationelle Selbstbestimmung. Insbesondere aufgrund der Anerkennung des allgemeinen Persönlichkeitsrechts nach Art. 2 I, Art. 1 I GG (sowie dessen Ausprägungen) als sonstiges Recht im Sinne des § 823 I BGB und des durch weitere Rechte, die an den Dateninhalt anknüpfen, vermittelten absoluten Schutzes an Daten (dazu sogleich) besteht keine Erforderlichkeit für die Anerkennung des eigenen Datenbestands als sonstiges Recht im Sinne des § 823 I BGB.

- Insolvenzrechtlicher und vollstreckungsrechtlicher Schutz

Der Rechtsinhaber kann im Falle einer Insolvenz derjenigen Stelle, die Daten des Rechtsinhabers gespeichert hat, ein Aussonderungsrecht gemäß § 47 InsO geltend machen und damit die Daten vor unbefugtem Zugriff schützen. Im Falle einer Zwangsvollstreckung kann der Rechtsinhaber eine Drittwiderspruchsklage gemäß § 771 ZPO erheben.

Ansprüche, die an den Dateninhalt anknüpfen Ansprüche, welche an den Dateninhalt anknüpfen, können aus unterschiedlichen rechtlichen Gesichtspunkten resultieren. Da die Rechtsordnung mehrere Anknüpfungspunkte für einen Schutz am Dateninhalt beinhaltet, kommt es für die Bestimmung der jeweiligen Schutzregime auf den jeweiligen Dateninhalt an. Insbesondere spielen hierbei

[29] Vgl. *Wagner*, in: MüKoBGB/, § 823 Rn. 294.
[30] Vgl. *Wagner*, in: MüKoBGB, § 823 Rn. 296.
[31] Vgl. am Beispiel von Domainnamen: BGH Urt. v. 18.1.2012 – I ZR 187/10 – NJW 2012, 2034 Rn. 23 f; *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 49.
[32] BGH Urt. v. 18.1.2012 – I ZR 187/10 – NJW 2012, 2034 Rn. 23.
[33] Siehe die Ausführungen in *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 50 f.

das Datenschutzrecht, das Immaterialgüterrecht und der Schutz von Betriebs- und Geschäftsgeheimnissen eine Rolle.[34]

- Datenschutzrecht

Im Anwendungsbereich des Datenschutzrechts werden personenbezogene Daten geschützt. In grundrechtlicher Hinsicht geht der hierdurch vermittelte Schutz auf das Recht auf Datenschutz gemäß Art. 8 GRCh, das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 7 GRCh und das Recht auf informationelle Selbstbestimmung gemäß Art. 1 I, Art. 2 I GG zurück. Neben anderen rechtlichen Bestimmungen, wie etwa der ePrivacy-Richtlinie bzw. der geplanten ePrivacy -erordnung, nationalen Regelungen (wie z. B. den Datenschutz im Arbeitsverhältnis betreffend) beinhaltet insbesondere die DSGVO Regelungen über die Verarbeitung personenbezogener Daten. Danach ist die Verarbeitung personenbezogener Daten im Grundsatz verboten und nur bei wirksamer Einwilligung der betroffenen Person bzw. bei Bestehen einer gesetzlichen Erlaubnis (wie etwa zur Erfüllung einer vertraglichen Pflicht gemäß Art. 6 I 1 lit. b DSGVO) rechtmäßig (sogenanntes Verbot mit Erlaubnisvorbehalt). Neben dem datenschutzrechtlich Verantwortlichen ist auch der Auftragsverarbeiter Adressat der datenschutzrechtlichen Rechte und Pflichten. Insbesondere in den Fällen, in denen die Datenverarbeitung auf eine Einwilligung der betroffenen Person gestützt wird, hat die betroffene Person mit dem Widerrufsrecht ein effektives Mittel, um ungewünschte Datenverarbeitung zu unterbinden. Darüber hinaus stehen der betroffenen Person auch in allen anderen Fällen Betroffenenrechte zu, wie etwa das sogenannte „Recht auf Vergessenwerden“ gemäß Art. 17 DSGVO, das Recht auf Auskunft gemäß Art. 15 DSGVO, das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO und das Widerspruchsrecht gemäß Art. 21 DSGVO. Verstöße gegen datenschutzrechtliche Pflichten können nach Art. 82 DSGVO Schadensersatzansprüche nach sich ziehen bzw. nach Art. 83 DSGVO mit Geldbußen sanktioniert werden. Die Normen der DSGVO können außerdem über § 823 II BGB und § 1004 BGB analog Schadensersatz- bzw. Unterlassungsansprüche auslösen.[35] Das allgemeine Persönlichkeitsrecht bildet außerdem ein sonstiges Recht i. S. d. § 823 I BGB und kann ebenfalls über § 1004 BGB analog Anspruchsgrundlage für Unterlassungsansprüche sein.[36]

- Immaterialgüterrechte

Weitere Rechte, die an den Dateninhalt anknüpfen, existieren im Bereich des Urheber-, Patent-, Marken- sowie des Designrechts. Im Folgenden wird exemplarisch auf das Urheberrecht näher eingegangen.[37] Das Urheberrecht gewährt dem Schöpfer eines Werks ein dem Eigentum ähnliches Recht an seinem Geisteswerk, wodurch insbesondere die Verbreitung des Werks durch den Urheber kontrolliert werden kann. Datenbanken werden im urheberrechtlichen Kontext in zweierlei Hinsicht geschützt. Datenbankwerke sind Sammelwerke, deren Elemente systematisch oder methodisch angeordnet und einzeln mithilfe elektronischer Mittel oder auf andere Weise zugänglich sind. § 4 II UrhG schützt die Auswahl und Anordnung der einzelnen Elemente der Datenbanken. Der Zugriff auf einzelne Daten fällt hierbei allerdings nicht unter den Schutz des § 4 II UrhG. Geschützt ist vielmehr ein unbefugter

[34] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 56.
[35] *Frenzel*, in: Paal/Pauly, DSGVO Art. 82 Rn. 20; *Quaas*, in: BeckOK DatenschutzR, Art. 82 Rn. 11.
[36] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 57.
[37] Angelehnt an *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 57 f.

Zugriff auf die Struktur einer Datenbank. Ferner beinhaltet das Urheberrecht nach den §§ 87a ff. UrhG einen Investitionsschutz. Datenbank in diesem Sinne ist die Sammlung unabhängiger Elemente, die systematisch oder methodisch angeordnet und einzeln mithilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Schutzgut ist hierbei eine Investition in Datenbankinhalte. Nach § 87b UrhG hat der Datenbankhersteller das ausschließliche Recht, die Datenbank insgesamt oder in (wesentlichen) Teilen zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben.

- Geschäfts- und Betriebsgeheimnisse

Der durch die Rechtsordnung vermittelte Schutz von innerbetrieblichem Wissen, Know-how und sonstigen nicht öffentlich zugänglichen Informationen eines Unternehmens gilt auch bei Geheimnissen in Gestalt digitaler Daten.[38] Unter Geschäfts- oder Betriebsgeheimnis versteht man jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll.[39] Regelungen zum Schutz von Geschäfts- und Betriebsgeheimnissen sind beispielsweise die Art. 17 ff. UWG, welche zudem noch als Schutzgesetze i. S. d. § 823 II BGB deliktsrechtliche Bedeutung erlangen und Ansprüche auf Schadensersatz, Unterlassung und Beseitigung nach den §§ 823 II 1004 BGB auslösen können. Darüber hinaus können in diesem Zusammenhang – unabhängig vom Schutz durch das UWG – Ansprüche wegen Verletzung des Eigentums am Unternehmen und Eingriffs in das Recht am eingerichteten und ausgeübten Gewerbebetrieb nach § 823 I BGB in Betracht kommen.[40] Darüber hinaus können Geheimnisse insbesondere durch vertragliche Bestimmungen durch die Vertragsparteien einem Schutz unterworfen werden. Führen die Erben die Geschäfte des Erblassers als seine Rechtsnachfolger weiter, so gilt der durch die Rechtsordnung vermittelte Schutz für diese auch fort.

4.1.2.3 Mögliche Vorteile durch ein etwaiges absolutes Recht an Daten?

Wie oben dargestellt, bietet das geltende Recht durch unterschiedliche Ansatzpunkte einen Schutz von Daten. Fraglich ist, ob damit auch Herausforderungen, welche im Zusammenhang mit dem digitalen Nachlass stehen, interessengerecht gelöst werden können. Namentlich sind dies Fragen zum Zugang, zum Ausschluss und der Verwertung von Daten des Erblassers durch die Erben.

Zugangsrechte der Erben: Erforderlichkeit eines absoluten Rechts an Daten zur Qualifikation von Daten als vermögensrechtliche Position?

Bislang war die Frage des Zugangs der Erben zu Daten, welche im Rahmen eines Accountverhältnisses des Erblassers erhoben und verarbeitet wurden, uneinheitlich beantwortet und barg damit eine gewisse Rechtsunsicherheit. Ausgangspunkt dieser Unsicherheit über die Vererbbarkeit von Daten ist der erbrechtliche Grundsatz, dass nur vermögensrechtliche Positionen vererbt werden können.[41]

[38] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 58.
[39] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 58.
[40] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 59.
[41] *Müller-Christmann*, in: BeckOK BGB, § 1922 Rn. 24.

Nichtvermögensrechtliche Rechtsverhältnisse sind damit in der Regel unvererblich, während vermögensrechtliche Beziehungen in der Regel vererblich sind.[42] Dies kann den Schluss nahelegen, dass Daten, welche durch das Vorliegen eines Vertragsverhältnisses mit einem Datenverarbeiter erhoben und verarbeitet werden, mangels Qualifikation als vermögensrechtliche Position grundsätzlich nicht vererbt werden können. Dabei kann in den unterschiedlichsten Fällen durchaus ein Interesse der Erben am Integritäts-, Geheimnis- und Verwertungsschutz von Daten bestehen, wie etwa bei Daten, welche Informationen über persönliche Vorlieben oder Wünsche beinhalten, welche zwar für den Datenverarbeiter wirtschaftlich uninteressant sind, für die Erben aber, ähnlich wie Schriftstücken mit Bezug zu persönlichen Verhältnissen des Erblassers (§ 2047 BGB) oder Familienpapieren und Familienbildern (§ 2373 S. 2 BGB), eine vermögensrechtliche Bedeutung zukommt.[43]

Um Zweifel über die Frage der Vermögensrelevanz auszuräumen, könnte einem etwaigen absoluten Recht an Daten eine vermögensrechtliche Relevanz beigemessen werden, um die grundsätzliche Vererbbarkeit von Daten zu untermauern und Zweifel an der Vererbbarkeit zu beseitigen. Neben dem Einwand, dass ein absolutes Recht nicht zwingend eine Vermögensrelevanz begründen muss, besteht aber auch seit der Entscheidung des BGH über den Zugang der Erben zu einem Facebook-Account[44] unter der geltenden Rechtslage keine Notwendigkeit hierfür. Zum einen bilden Daten – unabhängig von der soeben angesprochenen Entscheidung des BGH – aus verschiedenen Gründen in der gegenwärtigen digitalen Welt regelmäßig einen Vermögenswert ab, z. B. unter beruflichen, urheberrechtlichen oder vertragsrechtlichen Gesichtspunkten.[45] Zum anderen gehen nach der Rechtsprechung des BGH auch Rechtspositionen mit höchstpersönlichen Inhalten unabhängig von einem Vermögenswert auf die Erben über, wie sich aus § 2047 II und § 2373 2 BGB ergibt.[46] Die Ansicht, welche zwischen Daten mit vermögensrechtlichem Inhalt und Daten mit höchstpersönlichem Inhalt unterscheidet und nur ersteren eine Vererbbarkeit beimisst, ist mit dem BGH und der überwiegenden Ansicht abzulehnen.[47] Das Kriterium der Höchstpersönlichkeit ist sowohl bei analogen als auch bei digitalen Inhalten in gleicher Weise betroffen, weshalb es nicht einleuchtet, analoge Inhalte anders als digitale Inhalte zu behandeln.[48]

In Bezug auf Daten, welche auf Speichermedien gespeichert sind, welche im Eigentum bzw. Besitz des Erblassers sind, besteht das Zugangs- und Ausschlussrecht bereits unter geltendem Recht für die Erben in dem Maße fort, wie es durch das Eigentumsrecht bzw. das dem Besitz zugrunde liegende Rechtsverhältnis (z. B. Mietvertrag über Speichermedien) ausgestaltet ist. Vorteile in Bezug auf die Vererbbarkeit der Daten in der Form, dass Erben ein Zugangs- und Ausschlussrecht über diese erlangen, würden durch ein absolutes Recht an Daten nicht erreicht. Sofern die Vererbbarkeit von Daten vertragsrechtlich ausgeschlossen wird, indem beispielsweise nur ein befristetes persönliches Nutzungsrecht gewährt wird, könnte die vertrags- und urheberrechtliche Zulässigkeit eines solchen Ausschlusses zwar kritisch hinterfragt werden. Dreh- und Angelpunkt wäre aber wohl nicht die Frage

[42] *Müller-Christmann*, in: BeckOK BGB, § 1922 Rn. 24.
[43] Vgl. *Weichert*, Netzwerk Datenschutzexpertise, Postmortaler Datenschutz, S. 11.
[44] BGH, Urteil vom 12.7.2018 – III ZR 183/17 – NJW 2018, 3178
[45] Vgl. *Weichert*, Netzwerk Datenschutzexpertise, Postmortaler Datenschutz, S. 8 ff.
[46] BGH, Urteil vom 12.7.2018 – III ZR 183/17 – NJW 2018, 3178 (3182) Rn. 49.
[47] Siehe hierzu bereits oben, Kapitel 2.3.1.1 auf Seite 40; BGH NJW 2018, 3178 (3182) Rn. 48 m. w. N.
[48] BGH, NJW 2018, 3178 (3182) Rn. 50 m. w. N.

nach einem absoluten Recht an den Daten, sondern eben die AGB-rechtliche Zulässigkeit einer solchen vertraglichen Abrede, da diese auch bei einer Anerkennung eines absoluten Rechts im Fokus stünde.[49] Vor diesem Hintergrund darf zumindest stark bezweifelt werden, dass sich für die Erben Vorteile durch die Anerkennung eines absoluten Rechts an Daten ergeben würden.

Ausschluss- und Verwertungsrechte: Möglicher Schutzlücke aufgrund Unanwendbarkeit der DSGVO für Verstorbene?

Erben treten mit dem Erbfall grundsätzlich in die Vertragsverhältnisse des Erblassers ein und können die sich aus dem Vertrag ergebenden Rechte, wie z. B. den Zugang zu der IT-Infrastruktur und damit zu gespeicherten persönlichen Daten bzw. die Löschung solcher Daten, gegenüber der anderen Vertragspartei geltend machen. Sind Daten beispielsweise innerhalb eines Vertragsverhältnisses erhoben und verarbeitet worden, gehen die durch den Vertrag begründeten Rechte und Pflichten in Bezug auf die Daten auf die Erben über.

Trotz dieser Feststellungen können sich Schutzlücken möglicherweise insoweit ergeben, als es um Fragen bezüglich eines Ausschlussrechts der Erben bzw. des Verwertungsrechts des Datenverarbeiters (d. h. des datenschutzrechtlich Verantwortlichen) geht. Gemeint sind damit Fälle, in denen vertragliche Regelungen bezüglich etwaiger Auskunftsrechte, Löschungsansprüche und Rechte zur Datenverarbeitung für die Zeit nach Vertragsbeendigung fehlen bzw. nur teilweise vorliegen. Wird beispielsweise ein Vertrag mit einem Anbieter digitaler Dienste geschlossen, in welchem in Bezug auf die Zeit nach Vertragsbeendigung keine Aussage getroffen wird zu Fragen der weiteren Verwertung oder der Löschung von Daten durch den Dienstanbieter (d. h. den Verantwortlichen), so ist der Erblasser zu Lebzeiten über die vertraglichen Pflichten des Anbieters des digitalen Dienstes hinaus durch gesetzliche Regelungen geschützt. So können etwa Ansprüche auf Schadensersatz aus § 823 I BGB i. V. m. dem allgemeinen Persönlichkeitsrecht nach Art. 1 I, Art. 2 I GG und auf Unterlassung gemäß § 1004 BGB analog geltend gemacht werden; ferner stehen insbesondere datenschutzrechtliche Rechte dem Erblasser zu Lebzeiten zur Hand, während der Dienstanbieter spiegelbildlich den datenschutzrechtlichen Pflichten unterworfen ist.

All diese Rechte gelten jedoch nicht, wenn der Erblasser stirbt: Das Datenschutzrecht gilt laut Erwägungsgrund 27 S. 1 DSGVO nicht für die personenbezogenen Daten Verstorbener. Dies bedeutet, dass Erben folglich auch keine Ansprüche aus der DSGVO mehr durchsetzen können, wie z. B. Widerspruchs,- Auskunft- und Löschungsrechte. Entsprechendes gilt für Ansprüche aus §§ 823 I 1004 BGB i. V. m. dem Allgemeinen Persönlichkeitsrecht aus Art. 2 I, Art. 1 I GG, diese können nur lebenden Personen zustehen. Insoweit könnte eine Schutzlücke bestehen, d. h. bei fehlender Regelung über die weitere Datenverarbeitung personenbezogener Daten des Erblassers könnte der Datenverarbeiter (d. h. der etwaige datenschutzrechtlich Verantwortliche) ungeachtet der datenschutzrechtlichen Bestimmungen aus der DSGVO und damit ohne Beachtung etwaiger Betroffenenrechte die Daten des Erblassers weiter verarbeiten. Da die „Hergabe“ der Daten insbesondere bei Verträgen, in denen die datenschutzrechtliche Einwilligung die Gegenleistung für das Bereitstellen der IT-Infrastruktur darstellt,[50] nach Vorstellung der betroffenen Person wohl regelmäßig nur für die Dauer des Bestehens

[49] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 71.
[50] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 202.

des Vertrags beabsichtigt war, dürfte eine fortdauernde Datenverarbeitung über die Vertragsdauer hinaus nicht im Interesse der betroffenen Person sein.

Ein etwaiges absolutes Recht an Daten könnte derart gestaltet werden, dass durch die Ausschlussfunktion den Berechtigten (d. h. auch den Erben) Ansprüche auf Löschung der beim Dienstanbieter noch gespeicherten Daten bzw. auf Unterlassung weiterer Verarbeitung zustehen würden. Ansprüche könnten dementsprechend gemäß § 823 I (bei Anerkennung als sonstiges Recht) bzw. II, § 1004 BGB erwachsen. Bei Eintreten des Erbfalls könnten die Erben etwaige Verträge mit Dienstanbietern beendigen und sodann die Beseitigung der rechtswidrigen Datenverarbeitung in Form von Löschung bzw. Herausgabe der Daten verlangen. Spiegelbildlich könnte ein absolutes Recht an Daten die Verwertung durch die Erben sichern.

Fraglich ist jedoch, ob tatsächlich eine Schutzlücke besteht. Dies ist zu verneinen, wenn anderweitige Ausschluss- und Verwertungsrechte der Erben aufgrund der geltenden Rechtslage bestehen, die einen ausreichenden Schutz gewähren:

- Ansprüche aus Vertrag (bzw. ergänzender Vertragsauslegung) am Beispiel von Social Media und Cloud Computing

Bei entsprechender vertraglicher Regelung bestehen Ansprüche auf Herausgabe direkt aus dem Vertrag. Fehlt es an einer vertraglichen Regelung, so kommen Ansprüche aus dem einschlägigen gesetzlich geregelten Vertragsrecht sowie aus ergänzender Vertragsauslegung in Betracht. Beispielhaft wird im Folgenden auf Social-Media-Verträge sowie Cloud-Computing-Verträge eingegangen.

Bei Verträgen über die Mitgliedschaft in einem sozialen Netzwerk herrscht über deren vertragliche Einordnung keine Einigkeit. So werden etwaige Verträge bei Entgeltlichkeit als Miet-, Dienst- oder auch Werkverträge eingeordnet. Bei Unentgeltlichkeit soll nach einer Ansicht ein Auftragsverhältnis vorliegen, eine weitere Ansicht sieht auch hierin einen Dienstvertrag.[51] Gegen die Annahme eines Auftrags bzw. eines Dienstvertrages werden allerdings gewichtige Argumente angeführt. So fehle zum einen das für einen Auftrag erforderliche Tätigwerden im fremden Interesse, da nicht davon ausgegangen werden kann, dass die Weitergabe der personenbezogenen Daten des Nutzers als Kundenprofil der Werbeindustrie in seinem Interesse und damit in seinem Auftrag erfolgt. Zum anderen bedürfe es für eine Einordnung als Dienstvertrag einer Entgeltlichkeit, woran es regelmäßig fehle.[52] Vorzugswürdig erscheint die Ansicht, Social-Media-Verträge als einheitliche Austauschverträge anzusehen, wobei einerseits eine lizenzähnliche Einräumung der Nutzung personenbezogener Daten für Werbezwecke, die man als Miete oder Kauf qualifizieren könnte, andererseits die Einräumung der Nutzung der IT-Infrastruktur vorliegt, wobei man letztere als Kombination von §§ 535 ff. und §§ 611 ff. BGB begreifen kann.[53] Unter Beachtung der Vorschriften des betroffenen Vertragsteils würden bezogen auf die Nutzung der personenbezogenen Daten die miet- bzw. kaufrechtlichen Vorschriften zur Anwendung kommen. Bei Beendigung des Vertrages über die Nutzung des Social-Media-Netzwerks würde den Erben folglich ein Anspruch entsprechend § 546 BGB auf Rückgabe der Daten, was die Löschung der Daten beinhalten würde, zustehen.

[51] Vgl. die Ausführungen bei *Bräutigam*, MMR 2012, 635 (636).
[52] *Bräutigam*, MMR 2012, 635 (636).
[53] *Bräutigam*, MMR 2012, 635 (640.).

Aufgegriffen kann ferner insbesondere eine Herausgabepflicht aus ergänzender Vertragsauslegung. Ebenso wie der Nutzer von digitalen Diensten lediglich ein insoweit beschränktes Nutzungsrecht an der Nutzung der IT-Infrastruktur des Anbieters für den Zeitraum des Bestehens eines Vertrags mit diesem hat, kann der etwaige Erblasser nach §§ 133, 157 BGB erwarten, dass der Anbieter entsprechend für den gleichen Zeitraum ein Recht zur Datenverarbeitung erhält, ein solches Recht aber nicht über die Vertragsdauer hinaus gewährt werden soll. Für ein solches Verständnis spricht auch, dass etwaige Abreden dem Kopplungsverbot gemäß Art. 7 IV DSGVO standhalten müssen (s.o.), um die Einwilligung nicht als unwirksam ansehen zu müssen.

Insbesondere bei Cloud-Computing-Verträgen[54] werden Ansprüche aus § 667 BGB i. V. m. § 675 BGB, § 539 II BGB, § 242 BGB oder § 241 II BGB diskutiert. Zivilrechtlich kann bei Cloud-Computing-Verträgen oftmals von einer Zuordnung als Miet-, Dienst- oder Werkvertrag ausgegangen werden, sodass ein Anspruch aus §§ 667, 675 BGB nicht gegeben ist. Handelt es sich jedoch bei der Leistungspflicht des Cloudbetreibers um eine entgeltliche Verwaltung fremden Vermögens, so kann von einem Geschäftsbesorgungsvertrag nach § 675 BGB ausgegangen werden, sodass ein entsprechender Anspruch auf Herausgabe dann vorliegt.[55] Wie bei Verträgen über die Nutzung von Social-Media-Netzwerken auch kommt auch eine Herausgabepflicht aufgrund ergänzender Vertragsauslegung in Betracht. Eine solche Pflicht ergibt sich aus dem Interesse des Nutzers, jederzeit und insbesondere nach Vertragsbeendigung die Herausgabe der Daten verlangen zu können. Nach Vertragskündigung folgt dies als Nebenpflicht gemäß § 241 II BGB.[56]

- Anspruch der Erben aus § 812 I 2 Alt. 1 BGB

In Betracht kommt die Geltendmachung eines Anspruchs aus ungerechtfertigter Bereicherung gemäß § 812 I 2 Alt. 1 BGB.[57] Zu beachten ist hierbei, dass bei Bestehen speziellerer Rückabwicklungsansprüche (wie z. B. § 546 BGB) diese gegenüber Ansprüchen aus Kondiktion vorrangig sind.[58] Die folgenden Ausführungen sind dienen daher der Vollständigkeit der infrage kommenden Ansprüche.

Da die Erben in das Vertragsverhältnis des Erblassers eintreten, können sie unter den gleichen Bedingungen wie der Erblasser den Vertrag beendigen, z. B. durch Kündigung. Die Voraussetzungen des § 812 I 2 Alt. 1 BGB würden regelmäßig erfüllt: Mit den Daten des Erblassers hat der Anbieter des digitalen Dienstes regelmäßig einen Vermögenswert erlangt. Dies geschieht in der Regel durch bewusste und zweckgerichtete Mehrung fremden Vermögens, also durch Leistung des Erblassers. Durch die Beendigung des Vertrages durch die Erben ist auch der Rechtsgrund für die Speicherung und weitere Verarbeitung der Daten nachträglich entfallen. Der Bereicherungsanspruch ist auf Herausgabe des Erlangten gerichtet, dies beinhaltet zumindest die Möglichkeit zur Speicherung der Daten durch die Erben sowie den Verlust der Zugangsmöglichkeit durch den Datenverarbeiter. Damit besteht bereits nach geltender Rechtslage ein Anspruch der Erben auf Löschung der Daten beim Dienstanbieter (d. h. dem datenschutzrechtlich Verantwortlichen).

[54] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 161.
[55] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 162.
[56] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 162.
[57] Vgl. *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 35.
[58] *Wendehorst*, in: BeckOK BGB, § 812 Rn. 74.

Man könnte allerdings erwägen, dass ein solcher Anspruch nicht besteht, wenn der Erblasser dem Dienstanbieter zur Lebzeiten die weitere Nutzung der Daten nach Vertragsbeendigung erlaubt hat. Der Dienstanbieter hätte damit nach dem Tod des Erblassers weiterhin einen Rechtsgrund zur Datenverarbeitung in der Hand, ohne dass den Erben das Recht auf Widerruf gemäß Art. 7 III DSGVO zustünde, da die DSGVO nur für Daten lebender Personen Anwendung findet.[59] Da eine solche Erlaubnis zur weiteren Verarbeitung eine Einwilligung zur Datenverarbeitung darstellt, müssten allerdings die datenschutzrechtlichen Anforderungen an die Freiwilligkeit, insbesondere das Kopplungsverbot gemäß Art. 7 IV DSGVO, beachtet werden. Danach muss bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Da die Datenverarbeitung bei Beendigung des Vertrags nicht mehr für die Erfüllung des Vertrags erforderlich sein würde, würde dies bei der Beurteilung der Freiwilligkeit gegen das Vorliegen eben dieser sprechen. Zweifelhaft wäre zudem die AGB-rechtliche Zulässigkeit einer solchen Klausel, da bei Vorliegen eines einheitlichen Austauschvertrags die Vertragsbeendigung die Leistungspflicht der betroffenen Person aufhebt, eine Klausel, welche darüber hinaus eine Leistungspflicht begründet, als überraschend im Sinne des § 305c BGB qualifiziert werden könnte und damit nicht Vertragsbestandteil würde.[60] Ein Anspruch auf Herausgabe der Daten bzw. auf Löschung gemäß § 812 I 2 Alt. 1 BGB würde damit wohl auch bei Vorliegen einer solchen Klausel bestehen.

- Gesetzliche Ansprüche auf Sicherung von Geschäfts- und Betriebsgeheimnissen

Ansprüche, die Geschäfts- und Betriebsgeheimnisse sichern (dazu siehe die Ausführungen oben), sind an die Inhaberschaft von Unternehmen gekoppelt, d. h. etwaige Ansprüche gehen auf die Erben des Unternehmens über. Dies gilt sowohl für gesetzliche Ansprüche als auch für vertragliche Ansprüche. Insoweit stellen sich keine nennenswerten Probleme.

- Ansprüche aus Immaterialgüterrechten

Auch hier stellen sich keine nennenswerten Probleme, da Immaterialgüter vererbt werden können und die sich aus der Inhaberschaft des jeweiligen Immaterialgüterrechts (z. B. Urheberrechts) ergebenden Ansprüche (Ausschluss- und Verwertungsrechte) den Erben als neuen Inhabern zustehen.

- Eigene Ansprüche der Erben wegen Übergangs des Personenbezugs

Eigene datenschutzrechtliche Ansprüche der Erben können sich daraus ergeben, dass der Vertragspartner Kenntnis von der Erbenstellung erlangt und damit Daten der Erblassers nunmehr den Erben (als solchen) zugeordnet werden können, folglich zu personenbezogenen Daten der Erben werden.[61]

[59] Eine Beseitigung der Einwilligung mittels Ausübung des Widerrufsrechts durch die Erben kommt daher nicht in Betracht.

[60] Vgl. zur AGB-Kontrolle bei vorformulierten Einwilligungen Erwägungsgrund 42 S. 3 DSGVO.

[61] Eine Zuordnung der Daten als vermögensrechtlich relevant ist nicht erforderlich, da der Eintritt der Erben in den bestehenden Vertrag mit dem Erblasser dies nicht voraussetzt, vgl. oben.

Entsprechend könnten die Erben die Betroffenenrechte der DSGVO, z. B. das Recht auf Auskunft, Löschung, etc. durchsetzen.[62]

- Ansprüche aus postmortalem Persönlichkeitsrecht des Erblassers gemäß Art. 1 I GG

Eine Einschränkung in Bezug auf die Möglichkeit der weiteren Verarbeitung, etwa durch Anbieter digitaler Dienste, könnte sich außerdem aus der Beachtung des postmortalen Persönlichkeitsrechts des Erblassers ergeben. Eine Verletzung der vermögenswerten Bestandteile des Persönlichkeitsrechts kann zu einem Entschädigungsanspruch führen. Hierbei ist zu beachten, dass den Erben nicht ein uneingeschränktes positives Benutzungsrecht kennzeichnender Persönlichkeitsmerkmale wie z. B. des Namens oder des Bildnisses, das auch gegen den ausdrücklichen oder mutmaßlichen Willen des verstorbenen Trägers des Persönlichkeitsrechts eingesetzt werden könnte, zusteht. Vielmehr ist eine Nutzung der nach dem Tode bestehenden Vermarktungsmöglichkeiten nur unter Berücksichtigung dieses Willens möglich.[63] Zu beachten ist ferner, dass Ansprüche aus postmortalem Persönlichkeitsrecht nicht nur gegen etwaige Vertragspartner des Erblassers (wie z. B. Anbieter digitaler Dienste) sondern auch gegenüber den Erben bestehen können. Dies gilt namentlich bei Verletzung ideeller Bestandteile des Persönlichkeitsrechts. Insoweit können den nächsten Angehörigen Widerrufs- und Unterlassungsansprüche zustehen. Aus dem eben Gesagten folgt also nicht nur eine Beschränkung hinsichtlich der Datenverarbeitung für Anbieter digitaler Dienste, sondern u.U. auch für die Erben.[64]

Schaffung eines absoluten Rechts an Daten nicht zwingend erforderlich zum Schließen noch unbekannter Schutzlücken

Wie dargestellt, beinhaltet bereits das geltende Recht Möglichkeiten zum Zugang zu Daten sowie zur Verwertung und zum Ausschluss Dritter von Daten des Erblassers, die von den Erben in Anspruch genommen werden können. Eine Anerkennung eines absoluten Rechts an Daten würde etwaige Probleme hinsichtlich der Vererbbarkeit von Daten, insbesondere die AGB-rechtliche Problematik mit urheberrechtlich geschützten Inhalten, nicht zwangsläufig lösen.[65] Darüber hinaus steht es dem Gesetzgeber frei, Rechte in Bezug auf Daten von Verstorbenen einfachgesetzlich und mit weniger regulatorischem Aufwand zu schaffen, als es die Schaffung eines für die Rechtsordnung neuen absoluten Rechts an Daten erfordern würde. Zwar ist auch eine Anerkennung eines absoluten Rechts durch richterliche Rechtsfortbildung möglich, doch auch dann stellen sich vielerlei Fragen (etwa in Bezug auf Inhaberschaft, konkurrierende Rechte, etc.), deren Beantwortung sich über Jahre hinziehen würde.

Gemäß Erwägungsgrund 27 S. 2 DSGVO können die Mitgliedsstaaten Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen. Diese Öffnungsklausel ermöglicht damit den Mitgliedsstaaten durch Schaffung entsprechender nationaler Regelungen, beispielsweise datenschutzrechtliche Schutzinstrumente, die nach der DSGVO nur lebenden Personen zustehen, Erben an die Hand zu geben. So könnte beispielsweise geregelt werden, dass Betroffenenrechte wie etwa

[62] Vgl. *Weichert*, Netzwerk Datenschutzexpertise, S. 18 m. w. N.
[63] Vgl. oben; BGH I ZR 49/97 – „Marlene Dietrich" – GRUR 200, 709 (714).
[64] Vgl. *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 340.
[65] Diesbezüglich vgl. die Ausführungen in Kaptel 5.

das Auskunftsrecht, das Recht auf Löschung, etc. gleichermaßen den Erben zustehen und gegenüber dem Verantwortlichen geltend gemacht werden können. Im Vergleich zu der Begründung eines neuen absoluten Rechts an Daten erscheint diese Möglichkeit weniger regulatorischen Aufwand zu erfordern, da sich Fragen wie etwa bezüglich der Inhaberschaft oder der konkreten Wirkungen eines etwaigen absoluten Rechts an Daten und der damit verbundenen Ansprüche nicht stellen würden. Der Gesetzgeber ist bei der Schaffung neuer Regelungen in Bezug auf Rechte an personenbezogener Daten Verstorbener auch nicht an Vorgaben der DSGVO gebunden, da die DSGVO diesen Bereich ausdrücklich nicht regelt und damit auch nicht auf eine Vollharmonisierung abzielt.

Ähnliches kann auch in Bezug auf rechtliche Unklarheiten innerhalb des AGB-Rechts gefordert werden. In diesem Zusammenhang kann de lege lata insoweit von einer Schieflage für Verbraucher gesprochen werden, als die Vererbbarkeit urheberrechtlich geschützter digitaler Werte durch entsprechende AGB-Klauseln beschränkt oder aufgehoben wird.[66] Eine Anerkennung oder Schaffung eines absoluten Rechts an Daten würde diese Schieflage nicht aufheben, es bliebe letztlich bei der Frage der Wirksamkeit einer AGB-rechtlichen Beschränkung eines solchen Rechts.

4.1.3 Fazit

Ein etwaiges absolutes Recht an Daten bietet aus dem Blickwinkel des digitalen Nachlasses keine solchen Vorteile im Hinblick auf Fragen des Zugangs zu Daten des Erblassers sowie zu deren Verwertung und des Ausschlusses von Dritten durch die Erben, welche nicht auch bereits durch die bestehende Rechtsordnung bzw. anderweitige und weniger aufwendige Gesetzesänderungen interessengerecht erreicht werden können. Es stehen den Erben damit umfangreiche Ansprüche gegen Datenverarbeiter aus Vertrag sowie direkt aus dem Gesetz zu. Eine Anerkennung bzw. Schaffung eines absoluten Rechts an Daten zur Sicherung der Vererbbarkeit von Daten, zur Sicherung von Zugangs-, Ausschluss- und Verwertungsrechten, ist damit – im Kontext des digitalen Nachlasses – nicht zwingend erforderlich. Dementsprechend bedarf es auch keiner weitergehenden Analyse hinsichtlich der etwaigen konkreteren Ausgestaltung eines solchen absoluten Rechts an Daten.

4.1.4 Einräumung einer Lizenz an personenbezogenen Daten

Personenbezogene Daten dürfen nur dann durch einen Verantwortlichen verarbeitet werden, wenn eine Einwilligung der betroffenen Person vorliegt (Art. 6 I 1 lit. a DSGVO) oder ein gesetzlicher Erlaubnistatbestand (Art. 6 I 1 lit. b–f DSGVO) greift. Darüber hinausgehende Möglichkeiten, eine Datenverarbeitung zu legitimieren, sind in der DSGVO bzw. allgemein im Datenschutzrecht nicht vorgesehen. Vor allem kennt das Datenschutzrecht keine „Lizenzierung“ einer Datenverarbeitung, jedenfalls nicht unter diesem Begriff. Im Grunde bedeutet „Lizenz“ nicht mehr als eine Erlaubnis, Daten zu verarbeiten. Diese „Lizenz“ stellt die datenschutzrechtliche Einwilligung gemäß Art. 6 I 1 lit. a DSGVO bereits

[66] Vgl. Kapitel 5 auf Seite 115.

dar. Durch sie kann die betroffene Person eine konkrete Datenverarbeitung „lizenzieren“ bzw. erlauben. Der Erblasser könnte bereits zu Lebzeiten regeln, dass die ihn (zu Lebzeiten) betreffenden personenbezogenen Daten nach seinem Tod durch die Erben weiter verarbeitet werden dürfen. Insoweit erteilt der Erblasser eine Einwilligung in die Datenverarbeitung nach dem Tod. Zwar gilt das Datenschutzrecht nach dem Tod nicht mehr, trotzdem müssen aber die vorsorglichen Maßnahmen die Erben binden.[67]

4.2 Postmortaler Datenschutz

Nach dem Tod fehlt der verstorbenen Person jede Möglichkeit, lenkend auf das Verfahren mit den Daten einzuwirken. Wollen Verbraucher einem völligen Kontrollverlust über die Daten nach dem Tod vorbeugen, müssen sie bereits zu Lebzeiten selbst vorsorglich tätig werden. Voraussetzung dafür ist wiederum, dass sie hinsichtlich ihres digitalen Nachlasses sensibilisiert werden. Hierin liegt letztlich das größte Problem, das es zu beheben gilt: Die meisten Menschen wissen einfach nicht, was nach ihrem Tod mit den Daten passiert. Dabei hat es jeder Einzelne selbst in der Hand, das Verfahren mit den Daten nach dem Tod rechtssicher zu regeln.

Zwar ist das Datenschutzrecht nicht auf personenbezogene Daten Verstorbener anwendbar,[68] denn das Persönlichkeitsrecht und damit auch das Recht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts erlöschen mit dem Tod des Menschen.[69] Damit erklären der Gesetzgeber sowie die Gerichte allerdings nicht, dass den betroffenen Personen die Regelung des Umgangs mit den Daten nach ihrem Tod grundsätzlich verwehrt sein soll:

Für den Betroffenen wäre es nicht hinnehmbar, zu keinem Zeitpunkt zu wissen, was nach dem Tod mit den Daten passiert. Durch einen derartigen Kontrollverlust wären die betroffenen Personen bereits zu Lebzeiten im Umgang mit den sie betreffenden personenbezogenen Daten gehemmt.[70] Der Schutz von Daten nach dem Tod durch den Erblasser selbst ist ein integraler Bestandteil der Ausübung des Rechts auf informationelle Selbstbestimmung zu Lebzeiten.[71]

Der postmortale Datenschutz steht darüber hinaus in einem engen Zusammenhang mit dem – durch die BVerfG-Rechtsprechung[72] entwickelten – postmortalen Persönlichkeitsrecht:

- Der postmortale Persönlichkeitsschutz greift dabei bereits unabhängig von einer vorsorglichen Regelung des Erblassers. Die nächsten Angehörigen sind grundsätzlich berechtigt, Ansprüche, die auf den Schutz des postmortalen Persönlichkeitsrechts des Verstorbenen abzielen, geltend

[67] Dazu siehe nächstes Kapitel 4.2

[68] *Gola*, in: Gola, DSGVO, Art. 4 Rn. 26; s. Erwgr 27 S. 1 DSGVO.

[69] U. a. BVerfG, NJW 2001, 594; *Große-Boymann*, in: Burandt/Rojahn (Hrsg.), Erbrecht, § 1922 Rn. 70.

[70] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 364; *Martini*, JZ 2012, 1145 (1149f.).

[71] *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, 23; *Gola*, in: Gola, DSGVO, Art. 4 Rn. 29.

[72] Geschützt wird der allgemeine Achtungsanspruch, der dem Menschen kraft seines Personenseins zusteht: BGH, NJW 1968, 1773. Das postmortale Persönlichkeitsrecht leitet sich allein aus Art. 1 I GG ab. Es ist vom Recht auf informationelle Selbstbestimmung und vom allgemeinen Persönlichkeitsrecht gemäß Art. 2 I und Art. 1 I GG abzugrenzen. Der Schutz des allgemeinen Persönlichkeitsrechts und all seiner spezielleren Ausformungen kommt nur lebenden Personen zu.

zu machen.[73] Etwaige Abwehransprüche können die Angehörigen beispielsweise gegenüber den Erben geltend machen, soweit diese personenverschieden sind.[74]

- Die Erben[75] zielen – in Umsetzung des letzten Willens des Erblassers – auf den Schutz des allgemeinen Achtungsanspruches sowie den Schutz des Erblassers vor postmortalen Verfälschungen oder Ausspähungen ab.[76] Es geht insoweit um das Aufrechterhalten des Abbilds des Erblassers zu dessen Lebzeiten.[77]

Postmortaler Datenschutz setzt sich somit aus Elementen des Rechts auf informationelle Selbstbestimmung (Art. 2 I und Art. 1 I GG) sowie des postmortalen Persönlichkeitsrechts (nur Art. 1 I GG) zusammen. Umfassender postmortaler Datenschutz ist nur dann gegeben, wenn beide Elemente wirksam ineinandergreifen. Voraussetzung dafür ist einerseits, dass der Erblasser durch vorsorgliche Regelungen zu Lebzeiten einen gewissen postmortalen Schutz der Daten veranlasst hat. Andererseits muss dieser durch den Erblasser initiierte postmortale Schutz auch tatsächlich umgesetzt werden. Es versteht sich von selbst, dass der Erblasser den zu Lebzeiten initiierten Schutz nicht persönlich umsetzen kann.[78] Hierbei ist der Erblasser auf diejenigen angewiesen, die er zu Lebzeiten „beauftragt“ hat, den Schutz der Daten nach dem Tod zu besorgen.[79]

Hat der Erblasser hingegen keine vorsorglichen Maßnahmen getroffen, können die gesetzlichen Erben und/oder die nächsten Angehörigen lediglich unter Beachtung eines – in der Regel nur schwer feststellbaren – hypothetischen oder mutmaßlichen Willens des Verstorbenen handeln und den Schutz der Daten besorgen. Sind die Erben, welche gleichzeitig die nächsten Angehörigen sind, dem Erblasser nicht wohlgesinnt, besteht das Risiko, dass der Achtungsanspruch des Erblassers nach dem Tod erheblich beeinträchtigt wird. Denkbar wäre dies insbesondere in solchen Fällen, in denen der Verstorbene eine prominente, in der Öffentlichkeit stehende Person war. Für die Erben könnte es sich unter finanziellen Gesichtspunkten insoweit anbieten, etwaige Daten weiterzugeben bzw. zu vermarkten. Allein diese Gefahr zeigt, wie wichtig es ist, dass der Erblasser bereits zu Lebzeiten eine konkrete Verfahrensweise mit den Daten nach dem Tod vorsorglich regelt.

4.2.1 Schutz durch vorsorgliche Regelungen

Der Erblasser kann und sollte also bereits zu Lebzeiten das Verfahren mit den Daten nach dem Tod vorsorglich regeln. Vorsorgemaßnahmen, die bereits zu Lebzeiten im Hinblick auf eine Datenverarbeitung nach dem Tod getroffen werden und erst postmortal ihre Wirkung entfalten, sind grundsätzlich

[73] *Leipold*, in: MüKoBGB, § 1922 Rn. 38.
[74] *Herzog*, NJW 2013, 3745 (3750); *Sorge*, MMR 2018, 372 (376).
[75] Auch ihnen obliegt – unabhängig davon, ob sie Angehörige sind – grundsätzlich der Schutz des Persönlichkeitsrecht des Verstorbenen, s. *Heinemann/Heinemann*, DuD 2013, 242 (244).
[76] Nach *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, S. 23, wirkt der Umgang mit den Daten von Verstorbenen auf die Persönlichkeitsentfaltung von Lebenden zurück; *Herzog*, NJW 2013, 3745 (3749).
[77] *Klas/Möhrke-Sobolewski*, NJW 2015, 3473 (3476).
[78] S. *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, S. 22
[79] Nach *Herzog*, NJW 2013, 3745 (3749) werden die Rechte des Erblassers durch den „Beauftragten“ bzw. „Wahrnehmungsberechtigten“ treuhänderisch ausgeübt.

zulässig und auch bindend.[80] Die Unanwendbarkeit des Datenschutzrechts steht dem nicht entgegen.[81] Durch vorsorgliche Maßnahmen kann der Betroffene sein Recht auf informationelle Selbstbestimmung vollumfänglich und uneingeschränkt ausüben. Der Fokus liegt hier also nicht auf der Unanwendbarkeit des Datenschutzrechts nach dem Tod, sondern auf der Gewährleistung einer uneingeschränkten Ausübung des Rechts auf informationelle Selbstbestimmung zu Lebzeiten. Der Erblasser kann so verhindern, dass er einem Kontrollverlust über die Daten nach dem Tod erliegt, der sich bereits zu Lebzeiten auf seinen Umgang mit den Daten auswirkt.

Zwar besteht auch im Falle vorsorglicher Regelungen keine Garantie, dass die Erben oder andere zu Lebzeiten „beauftragte“ Personen mit den Daten entsprechend des letzten Willens verfahren,[82] allerdings sinkt das Risiko erheblich, dass willkürlich und unter Beeinträchtigung des nach dem Tod fortwirkenden Achtungsanspruchs des Verstorbenen mit den Daten verfahren wird:

- **Schutz durch vorsorgliche Regelungen:** In Ausübung ihres Rechts auf informationellen Selbstbestimmung können Verbraucher bereits zu Lebzeiten regeln, was nach dem Tod mit den Daten passieren soll. Diese Regelungen können beispielsweise in einem Zweiparteienverhältnis (Erblasser und Verantwortlicher/Dienstanbieter) auf vertraglicher Basis erfolgen oder auf klassischem Wege im Rahmen einer letztwilligen Verfügung bzw. eines Testaments. In letzterem Fall sind mindestens zwei Parteien (Erbe und Verantwortlicher/Dienstanbieter) in die tatsächliche Umsetzung des letzten Willens des Erblassers involviert. Beide Vorsorgemöglichkeiten haben ihre Vor- und Nachteile,[83] letztlich hängt die Wahl der vorsorglichen Maßnahme davon ab, was der Erblasser konkret regeln will (nur Regelung von Abwehransprüchen, wie Löschung/Sperrung, oder auch Regelung einer postmortalen Datenweitergabe an Dritte usw.). Möglich ist auch die Erteilung einer postmortalen Vollmacht, durch die dem Bevollmächtigten unabhängig von der Erbenstellung die Befugnis eingeräumt werden kann, das Verfahren mit den Daten des Erblassers nach dem Tod zu regeln.[84]

- **Gefahr einer erheblichen Beeinträchtigung des Achtungsanspruches:** Veranlasst der Erblasser zu Lebzeiten keinen Schutz durch vorsorgliche Maßnahmen, erhalten grundsätzlich erstmal die (gesetzlichen) Erben Zugriff auf die Daten.[85] Die Erben können mit diesen Daten nach freiem Ermessen verfahren, sie sind nicht mehr an datenschutzrechtliche Bestimmungen oder ähnliches gebunden. Ihnen obliegt zwar der Schutz des Achtungsanspruchs des Erblassers, eine überprüfbare Verpflichtung der Erben, diesen Achtungsanspruch auch tatsächlich zu schützen, besteht allerdings nicht.[86]

[80] Siehe auch *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 364.

[81] So aber beispielsweise *Martini*, JZ 2012, 1145 (1148), der meint, dass Vorsorgemaßnahmen, wie beispielsweise die Löschung der Daten nach dem Tod, nicht bindend seien, da das Datenschutzrecht nach dem Tod nicht mehr gelte. Diese Ansicht kann allerdings nicht überzeugen. Eine derartige Unverbindlichkeit der Vorsorgemaßnahmen hätte zur Folge, dass die Betroffenen ihr Recht auf informationelle Selbstbestimmung zu Lebzeiten nicht uneingeschränkt ausüben können.

[82] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 366.

[83] Siehe hierzu Kapitel 6.4.4.2 auf Seite 191.

[84] *Leipold*, in: MüKoBGB, § 1922 Rn. 47; dazu ausführlicher in der Studie Kapitel 6.3 auf Seite 180.

[85] BGH, NJW 2018, 3178.

[86] Falls die Erben und die nächsten Angehörigen personenverschieden sind, könnten die Angehörigen (als Kontrollinstanz und Wahrnehmungsberechtigte des postmortalen Persönlichkeitsschutzes des Verstorbenen) gegenüber den Erben

4.2.2 Vertragliche Regelungen mit dem Dienstanbieter

Verbraucher könnten das Verfahren mit den Daten nach dem Tod vertraglich mit dem konkreten Dienstanbieter regeln. Das Vertragsrecht ist vor dem Hintergrund der Privatautonomie offen für die lebzeitige Regelung von Maßnahmen, die auf einen postmortalen Datenschutz abzielen. So könnte im Rahmen vorsorglicher Maßnahmen beispielsweise geregelt werden, dass alle Daten – ohne zwischenzeitlichen Zugriff von Erben – nach dem Tod rückstandslos gelöscht werden.[87] Eine solche Vereinbarung mit einem Dienstanbieter könnte individualvertraglich oder in AGBs erfolgen, wobei in der Praxis hier nur die Regelung in AGBs infrage kommen wird. Individualvertragliche Regelungen sind im Online-Bereich nicht oder nur äußerst selten anzutreffen. In diesem Zusammenhang besonders hervorzuheben sind Regelungen, wie sie der Dienstanbieter Xing in seine AGBs aufgenommen hat. So erklärt dieser:

„Im Falle Ihres Ablebens können Ihre rechtlichen Erben auf Anforderung Einsicht in Ihre Xing-Profildaten erhalten. Sie können hier jedoch bestimmen, dass Ihre XING-Daten nicht vererbt, sondern stattdessen gelöscht werden sollen.“[88]

Der Dienstanbieter weist damit zunächst auf die geltende Rechtslage hin. Ferner stellt der Dienstanbieter dem Nutzer die (in seiner Wirkung relativ pauschale) Möglichkeit zur Wahl, zu bestimmen, dass alle Daten nach dem Tod gelöscht werden sollen. Durch derartige Regelungen wird dem Erblasser auf einfache Weise ermöglicht, bereits zu Lebzeiten das Verfahren mit den Daten nach dem Tod, unter Ausschluss jeden Zugriffes durch beispielsweise Erben, in verbindlicher Weise festzulegen. Solche Vereinbarungen nehmen eine Vorbildfunktion ein, insbesondere mit Blick auf die gesetzgeberische Regelung von Informationspflichten, die dem Dienstanbieter auferlegt werden sollten.[89] Von der Arbeitsgruppe „Digitaler Neustart“ wird diesbezüglich argumentiert, dass eine Hinweispflicht auf die Rechtslage im Zivil- bzw. Erbrecht grundsätzlich nicht vorgesehen sei und auch nicht verlangt werden könne. Wer sich über die geltende Rechtsage im Unklaren sei, könne sich Rechtsrat einholen.[90]

Diese Argumentation überzeugt nicht. Zunächst handelt es sich bei dem beispielhaft aufgeführten Hinweis nicht nur um einen Hinweis auf die zivil- bzw. erbrechtliche Rechtslage, sondern auch auf den postmortalen Datenschutz betreffende Gegebenheiten. Nach Erwgr 60 S. 1 DSGVO machen es die Grundsätze einer fairen und transparenten Verarbeitung erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Einhaltung von Informationspflichten kommt eine fundamentale Bedeutung zu, insbesondere mit Blick auf die Geltendmachung von Betroffenenrechten.[91] Klar ist: Diese Grundsätze gelten zunächst einmal im

ggf. Abwehransprüche geltend machen und somit den Achtungsanspruch des Verstorbenen auch nach dem Tod wahren. Eine externe Kontrollinstanz ist dann nicht ersichtlich, wenn Erben und Angehörige in einer Person vereint sind und der Erblasser sonst nichts geregelt hat.

[87] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 366; *Herzog*, Digitaler Nachlass, 258 ff., in: Kroiß/Horn/Solomon, Nachfolgerecht, Rn. 81; *Leipold*, in: MüKoBGB, § 1922 Rn. 42.

[88] Xing, https://faq.xing.com/de/einstellungen/ihr-xing-profil-nach-dem-tod.

[89] Siehe dazu (eher ablehnend) *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 367.

[90] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 364.

[91] *Schmidt-Wudy*, in: BeckOK Datenschutzrecht, Art. 13 Rn. 2.

Anwendungsbereich der DSGVO, also für die Daten von Lebenden. Allerdings müssen sie gleichzeitig auch für die Verarbeitung von Daten nach dem Tod der betroffenen Person in entsprechender Weise gelten: Nur wenn der Erblasser umfassend darüber informiert ist, was mit den Daten nach dem Tod passiert, kann er das Verfahren mit den Daten nach dem Tod selbstbestimmt und konkret ausgestalten.

Der Gesetzgeber sollte Dienstanbieter also verpflichten,[92] die Nutzer bereits bei Eröffnung des Accounts oder auch noch nach Vertragsschluss auf ihren digitalen Nachlass hinzuweisen. Diese Hinweispflicht könnte eine besonders effektive Form einer Sensibilisierung der Verbraucher hinsichtlich der Regelung ihres digitalen Nachlasses darstellen. Als gesetzlicher Mindeststandard könnte den Dienstanbietern aufgetragen werden, dass sie zunächst auf die geltende Rechtslage seit dem BGH-Urteil zu Facebook[93] hinweisen. Den Verbrauchern sollte transparent und in unmissverständlicher Weise aufgezeigt werden, dass bei fehlender Vorsorge die Erben grundsätzlich Zugang zu den Daten erhalten. Weiterhin bietet es sich an, dem Verbraucher eine pauschale Möglichkeit zur Löschung und/oder zur Weitergabe der Daten bereitzustellen.[94] Solche pauschalen Hinweise in Bezug auf die Löschung, Weitergabe bzw. Erhaltung von Daten, reichen aus, um die betroffenen Personen – in der Regel erstmals – auf das Thema des digitalen Nachlasses aufmerksam zu machen. Allein dieses erstmalige Aufmerksamkeitsmoment wäre ein nicht zu unterschätzender Erfolg einer gesetzlich festgelegten Informationspflicht. Die Auswahl, welche Möglichkeiten die Dienstanbieter tatsächlich anbieten wollen, sollte in ihr Ermessen gestellt werden.[95] Damit der Verbraucher nicht irrig davon ausgeht, dass lediglich der Übergang des Accounts samt Daten auf die Erben und beispielsweise eine vollständige Löschung der Daten nach dem Tod möglich sind, sollte weiterhin ein Hinweis auf weitergehende und weitaus differenzierte Möglichkeiten erfolgen, den digitalen Nachlass zu regeln. Diesbezüglich wird unter anderen von *Kühling/Martini* vorgeschlagen, dass die Informationspflichten für den Verantwortlichen ergänzt werden sollten. Demnach solle darüber informiert werden, dass „die Nutzer die Möglichkeit haben, Regelungen für die Verwendung ihr personenbezogenen Daten nach dem Tod zu treffen."[96] Hier wird man wohl darauf verzichten müssen, dass die Dienstanbieter sämtliche Möglichkeiten dem Verbraucher aufbereiten müssen, insoweit würde in die Vertragsfreiheit der Dienstanbieter übermäßig eingegriffen. Ausreichend wäre beispielsweise ein Hinweis in der Form, dass weitergehende Regelungen insbesondere im Rahmen eines Testaments oder einer Bevollmächtigung getroffen werden können.[97]

Die Regelung von Informationspflichten hinsichtlich einer Datenverarbeitung post mortem würde auch unter die Öffnungsklausel gemäß Erwgr 27 S. 2 DSGVO fallen.[98] Demnach können die Mitgliedsstaaten Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen. Die entsprechenden Hinweise des Dienstanbieters würden sich ausschließlich auf die Verarbeitung der Daten nach dem Tod beziehen.[99]

[92] Zu den Möglichkeiten, die Dienstanbieter freiwillig bereitstellen könnten, siehe Kapitel 7 auf Seite 291.
[93] BGH, NJW 2018, 3178; auf den BGH Bezug nehmend LG Münster, MDR 2019, 1067.
[94] *Leipold*, in: MüKoBGB, § 1922 Rn. 49; *Martini/Kienle*, JZ 2019, 235 (241)
[95] Zu den weiteren Möglichkeiten des Dienstanbieters siehe Kapitel 7 auf Seite 291.
[96] *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, 24.
[97] Zu den weiteren Möglichkeiten siehe Kapitel 7 auf Seite 291.
[98] *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, 24.
[99] Vgl. *Kühling/Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, S. 24.

Geht es dem Erblasser vor allem darum, dass nach seinem Tod niemand Zugriff auf sensible Daten erhält, liegen die Vorteile einer vertraglichen Regelungen auf der Hand. Sie überzeugt vor allem durch ihre Praktikabilität: Eher beschäftigen sich Verbraucher mit einer kurzen, standardmäßigen AGB-Klausel, als mit den vielen verschiedenen Möglichkeiten einer Testamentserstellung. Durch eine Regelung mit dem Vertragspartner kann zudem die Kenntnisnahme von Außenstehenden, wie beispielsweise Angehörigen bzw. Erben, von vornherein ausgeschlossen werden. In die Umsetzung des letzten Willens wäre dann nur der Dienstanbieter involviert.

Hierin könnte allerdings gleichzeitig ein Nachteil bzw. ein Risiko einer nur vertraglichen Regelung mit dem Dienstanbieter liegen. Allseits bekannt ist der Wert von personenbezogenen Daten für Unternehmen. Durch den Tod verlieren die Daten zwar ihren Personenbezug, aber nicht zwangsläufig ihren Wert. Auch aus Daten Verstorbener können wertvolle Rückschlüsse gezogen werden. Steht die Löschung der Daten nur im vertraglich festgelegten Ermessen des Dienstanbieters, stellt sich die Frage, welche Instanz tatsächlich kontrollieren soll bzw. kann, ob der letzte Wille umgesetzt wurde.

Ein weiterer Nachteil ist, dass die rückstandlose Löschung von Daten viel zu pauschal ist. So wird es einem Erblasser meist nur um die Löschung von konkreten (besonders sensiblen) Daten und nicht von sämtlichen Daten gehen. Zudem könnte der Erblasser auch regeln wollen, dass die Daten an bestimmte Personen weitergegeben werden sollen (also positive Nutzung statt Löschung oder Sperrung). Erkennt der Erblasser schon zu Lebzeiten, dass seine Daten auch nach dem Tod einen gewissen Wert haben werden, könnte er auch einer weiteren Vermarktung beispielsweise durch die Angehörigen oder Erben zustimmen wollen. Solche ausdifferenzierten Regelungen werden im Rahmen von AGBs nicht möglich sein. Hier bieten beispielsweise testamentarische Regelungen einige Vorteile. Wollen die betroffenen Personen das Verfahren mit den Daten nach dem Tod weniger pauschal regeln, werden sie sich weitergehend mit dem Thema beschäftigen müssen und dies im Zweifelsfall dann auch tun. Sinn und Zweck einer hier vorgeschlagenen Informationspflicht ist lediglich eine effektive Sensibilisierung der Verbraucher. Die Informationspflicht der Dienstanbieter soll die Nutzer eines Online-Dienstes dazu bringen, sich mit den Fragen des digitalen Nachlasses möglichst frühzeitig auseinanderzusetzen.

4.2.3 Regelungen im Rahmen letztwilliger Verfügungen

Im Falle einer testamentarischen Regelung[100] sind die Erben gehalten, das letztwillig durch den Erblasser geäußerte Verfahren mit den Daten umzusetzen. Beispielsweise könnte der Erblasser im Testament regeln, dass die Erben eine Löschung sämtlicher Daten bei einem bestimmten Online-Dienst herbeiführen sollen, oder dass die Erben die Daten an jemanden Drittes weitergeben sollen.

Das Erbrecht ist insoweit offen für eine Regelung vorsorglicher Datenschutzmaßnahmen, als hier die Testierfreiheit gemäß Art. 14 GG gilt. Klassischerweise könnte der Erblasser seinen digitalen Nachlass im Rahmen eines Testaments regeln und die Erben beauftragen in einer bestimmten Art und

[100] Möglich ist neben der testamentarischen Regelung auch die Erteilung einer postmortalen Vollmacht. Zu den Vorteilen einer letztwilligen Verfügung gegenüber einer solchen Vollmacht siehe insbesondere Kapitel 6.4.4.2 auf Seite 191.

Weise mit den Daten zu verfahren.[101] Hier bietet sich beispielsweise die Erteilung von Auflagen im Testament an.[102] So könnte der Erblasser den Erben freistellen, ob sie bestimmte Daten zu kommerziellen Zwecken an Dritte weitergeben. Auch eine solche Regelung in einem Testament ist letztlich nur Ausdruck einer uneingeschränkten Ausübung der informationellen Selbstbestimmung zu Lebzeiten.

Grundsätzlich – auch ohne Regelung des Erblassers – erhalten die Erben Zugang zum Account und zu den dort enthaltenen den Daten des Erblassers.[103] Damit die Erben das testamentarisch geregelte Verfahren mit den Daten auch tatsächlich umsetzen können, bedarf es verschiedenster Durchsetzungsmechanismen. Möglich wäre beispielsweise, dass die Erben bereits als neuer Vertragspartner des Online-Dienstes eine Löschung der Daten besorgen könnten. Sind solche Ansprüche vertraglich nicht vorgesehen, kommen Abwehransprüche, insbesondere Auskunfts- und Löschungsansprüche[104] in Betracht.

Das wohl größte Problem im Rahmen letztwilliger Verfügungen ist die fehlende Prakitkabilität und Schnelligkeit im Rechtsverkehr. So können bereits Probleme auftreten, wenn es um die Frage geht, wie die Erben ihre Legitimation nachweisen können.[105] Im Falle der Einsetzung mehrerer Erben können zudem Streitigkeiten über die Auslegung des letzten Willens eine tatsächlich Umsetzung erheblich verzögern. In der Folge könnte der Achtungsanspruch des Erblassers erheblich beeinträchtigt werden. Zudem können sich auch im Verhältnis Erben und Dienstanbieter Schwierigkeiten ergeben, gerade, wenn es um die Frage geht, welche Rechte die Erben denn nun in Bezug auf die Daten haben. Vorteil einer testamentarischen Regelung ist allerdings die Möglichkeit, eine externe Kontrollinstanz, die die Umsetzung des letzten Willens überwacht, einzusetzen. Die Rede ist hier entweder von einem Testamentsvollstrecker oder einem Bevollmächtigten.[106]

4.2.4 Schutzerhöhende Maßnahmen

Der postmortale Schutz der Daten kann durch den Erblasser selbst initiiert werden. Die Umsetzung des postmortalen Schutzes obliegt den Erben, nächsten Angehörigen, Vertragspartnern oder anderen Wahrnehmungsberechtigten. Zur Kontrolle der tatsächlichen Umsetzung bedarf es externer Kontrollinstanzen. Die nächsten Angehörigen könnten beispielsweise die Umsetzung des letzten Willens durch die Erben überwachen.[107] Dies gilt jedenfalls, solange sie nicht selbst Erben sind.

Datenschutzbehörden kommen als kontrollierende Stelle nicht infrage. Sie sind gemäß Art. 51 I DSGVO für die Überwachung der Anwendung der DSGVO zuständig. Damit wird den Datenschutzbehörden

[101] *Steiner/Holzer*, ZEV 2015, 262 (266).
[102] *Leipold*, in: MüKoBGB, § 1922 Rn. 47.
[103] BGH, NJW 2018, 3178; auf den BGH Bezug nehmend LG Münster, MDR 2019, 1067.
[104] In Bezug auf Auskunftsansprüche: *Heinemann/Heinemann*, DuD 2013, 242 (244).
[105] *Lange/Holtwiesche*, Der digitale Nachlass, in: Bär/Grädler/Mayr, Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, 103 (115f.).
[106] Dazu ausführlicher in Kapitel 6.4.4.1 auf Seite 189.
[107] Entsprechende Ansprüche leiten sich aus dem postmortalen Persönlichkeitsrecht ab; so auch *Herzog*, Digitaler Nachlass, 258 ff., in: Kroiß/Horn/Solomon, Nachfolgerecht, Rn. 52.

allerdings nur die Überwachung der Verarbeitung personenbezogener Daten von natürlichen bzw. lebenden Personen aufgetragen.[108] Ohnehin wären die Datenschutzbehörden ressourcentechnisch völlig überfordert, wenn nun auch noch postmortal Datenverarbeitungen überwacht werden sollen.

Zielführend könnte die Einsetzung eines Testamentsvollstreckers sein, der die tatsächliche Umsetzung des letzten Willens des Erblassers überwacht.[109] Er wäre damit ein persönlicher „postmortaler Datenschutzbeauftragter".[110] Damit eine tatsächliche Umsetzung durch den Testamentsvollstrecker auch gewährleistet ist, müssten diesem Kontrollrechte, wie bspw. Auskunftsansprüche sowie etwaige Durchsetzungsmechmanismen, wie beispielsweise Löschungsansprüche, zugestanden werden. Die Ernennung des Testamentsvollstreckers ist selbstverständlich nur zu Lebzeiten möglich und müsste als vorsorgliche Maßnahme durch den Erblasser getroffen werden.

4.2.5 Kontrollverlust über die Daten

Hat der Erblasser keine vorsorglichen Maßnahmen getroffen, erhalten grundsätzlich die Erben Zugriff auf die Daten nach dem Tod.[111] Sind die Erben gleichzeitig die Angehörigen des Verstorbenen, gelangen die Daten insoweit in einen rechtsfreien Raum, als niemand überprüft bzw. zu überprüfen imstande ist, zu welchen Zwecken die Daten womöglich (von den Erben oder von Dritten) weiterverwendet werden. Diese Überprüfung ist gesetzlich auch schon gar nicht vorgesehen, das Datenschutzrecht gilt mit dem Tod der betroffenen Person nicht mehr, Datenschutzbehörden sind nicht zuständig. Sorgt der Erblasser nicht vor, besteht die Gefahr einer erheblichen Beeinträchtigung des über den Tod hinauswirkenden Achtungsanspruchs.

4.3 Zusammenfassung

Die Forderung nach einem absoluten Recht an Daten erscheint im Kontext des digitalen Nachlasses nicht begründet, da die bestehende Rechtsordnung unter Berücksichtigung höchstrichterlicher Rechtsprechung in ausreichender Weise Zugangs-, Ausschluss- und Verwertungsrechte der Erben gewährleistet.

Postmortaler Datenschutz ist unter der bestehenden Rechtslage möglich. Erblasser können bereits zu Lebzeiten das Verfahren mit den Daten nach dem Tod regeln und so einem völligen Kontrollverlust vorbeugen. Diese Möglichkeit entspringt dem zu Lebzeiten bestehenden Recht auf informationelle Selbstbestimmung. Um auch wirklich sicherzustellen, dass der Wille des Erblassers beachtet wird,

[108] Vgl. Erwgr 27 S. 1 DSGVO.

[109] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 366; vgl. auch *Bierman*, in: Scherer, Münchener Anwaltshandbuch, Rn. 77; *Leipold*, MüKoBGB, § 1922 Rn. 47.

[110] Vgl. hierzu bereits *Heinemann/Heinemann*, DuD 2013, 242 (244), wobei hier auf einen Schutz durch den „Datenschutzbeauftragten" abgestellt wird und nicht auf eine bloße Überwachung/Kontrolle der Umsetzung des letzten Willens des Erblassers.

[111] BGH, NJW 2018, 3178.

sollte über Kontrollinstanzen nachgedacht werden. Hier bietet sich zu Lebzeiten vor allem die Ernennung eines Testamentsvollstreckers an.

Effektiver postmortaler Datenschutz ist allerdings nur dann möglich, wenn die Verbraucher bzw. Nutzer eines Online-Dienstes ein gewisses Bewusstsein für ihren digitalen Nachlass entwickeln. Dieses Bewusstsein kann insbesondere durch eine – neu zu schaffende – gesetzliche Verpflichtung der Dienstanbieter, die Nutzer auf ihren digitalen Nachlass hinzuweisen und entsprechende Wahlmöglichkeiten bereitzustellen (beispielsweise Löschung von Daten), gestärkt werden.

Die Erben und auch die nächsten Angehörigen können nach dem Tod des Erblassers ebenfalls für einen Schutz der Daten sorgen, dies garantiert das postmortale Persönlichkeitsrecht. Dies gilt auch, wenn der Erblasser keinerlei Regelungen zu Lebzeiten getroffen hat. Dann kommt es vor allem auf den mutmaßlichen Willen des Erblassers an, soweit sich ein solcher ermitteln lässt. Hat der Erblasser keine vorsorglichen Regelungen zu Lebzeiten getroffen, stehen die Daten beispielsweise den Erben im Rahmen des Zugangsanspruches zum Account zur (freien) Verfügung. Eine Kontrollinstanz, die überprüfen könnte, ob die Erben den Achtungsanspruch des Erblassers wahren, ist beispielsweise in den nächsten Angehörigen zu sehen, soweit sie nicht mit den Erben in Personalunion zusammenfallen. In diesem – nicht sehr unwahrscheinlichen – Fall sind weitere Verarbeitungen der Daten nicht mehr überprüfbar. Diese fehlende Überprüfbarkeit sowie die damit einhergehende freie Verfügbarkeit der Daten nach dem Tod verdeutlichen die Relevanz der Regelung des digitalen Nachlasses zu Lebzeiten durch den Erblasser.

Das Wichtigste in Kürze

- Die Anerkennung bzw. Schaffung eines absoluten Rechts an Daten ist aus dem Blickwinkel des digitalen Nachlasses nicht erforderlich.

- Den Erben stehen nach geltendem Recht umfangreiche Befugnisse zu, um Zugang zu Daten des Erblassers zu erhalten, diese Daten zu nutzen und Dritte von der Nutzung auszuschließen.

- Der Schutz von Daten nach dem Tod ist möglich. Das Recht auf informationelle Selbstbestimmung und das postmortale Persönlichkeitsrecht bilden gemeinsam die rechtliche Grundlage für einen wirksamen postmortalen Datenschutz.

- Effektiver postmortaler Datenschutz ist nur dann möglich, wenn die Verbraucher bzw. Nutzer eines Online-Dienstes ein gewisses Bewusstsein für ihren digitalen Nachlass entwickeln. Dieses Bewusstsein kann insbesondere durch eine – neu zu schaffende – gesetzliche Verpflichtung der Dienstanbieter, die Nutzer auf ihren digitalen Nachlass hinzuweisen und entsprechende Wahlmöglichkeiten bereitzustellen (beispielsweise Löschung von Daten), gestärkt werden.

- Postmortaler Datenschutz setzt ferner ein Tätigwerden des jeweiligen Nutzers voraus. So kann vor allem durch vertragliche Regelungen, letztwillige Verfügungen oder eine postmortale Bevollmächtigung ein absoluter Kontrollverlust über die

Daten nach dem Tod vermieden werden. Fehlt es an vorsorglichen Maßnahmen, besteht das Risiko, dass der auch nach dem Tod fortwirkende Achtungsanspruch des Verstorbenen erheblich beeinträchtigt wird.

» Wirksamer postmortaler Datenschutz setzt schließlich auch immer ein Tätigwerden derer voraus, die durch den Erblasser „beauftragt“ wurden, mit den Daten in einer bestimmten Art und Weise zu verfahren. Um zu gewährleisten, dass dem letzten Willen des Verstorbenen auch tatsächlich Folge geleistet wird, bietet sich die vorsorgliche Einsetzung einer externen Kontrollinstanz an (beispielsweise im Rahmen des Testaments die Einsetzung eines Testamentsvollstreckers).

5 Untersuchung potenzieller Benachteiligungen der Verbraucher

Dieses Kapitel untersucht

- die Allgemeinen Geschäftsbedingungen (AGB) großer Anbieter digitaler Werte in Bezug auf Ausführungen zum digitalen Nachlass,
- die Vererbbarkeit digitaler Werte als Grundlage der Bewertung von AGB,
- die Rechtskonformität von AGB zum digitalen Nachlass,
- mögliche Benachteiligungen von Verbrauchern bei der Nutzung von Diensten, im Rahmen derer digitale Werte entstehen und/oder genutzt werden,
- Verbesserungsmöglichkeiten rund um den digitalen Nachlass aus Sicht der Verbraucher.

5.1 Relevanz Allgemeiner Geschäftsbedingungen

Zu den digitalen Werten gehören u. a. E-Books, digitale Musikdateien, erkaufte oder erspielte Spielstände in Spielkonsolen sowie digitale, personenbezogene Daten wie Fotos, geschriebene Beiträge und „Likes“. Die Grundlage der Nutzung solcher digitalen Werte bei einem bestimmten Anbieter bzw. auf einer bestimmten Online-Plattform bilden i. d. R. die sogenannten Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Anbieters. Bei AGB handelt es sich um Vertragsbestimmungen, die für eine Vielzahl von Verträgen vorformuliert wurden und von einer Vertragspartei der anderen Vertragspartei unterbreitet werden. AGB unterstützen also den schnellen und unkomplizierten Vertragsschluss zwischen Anbieter und Verbraucher, da die beiden Vertragsparteien keinen individuellen Vertrag aushandeln müssen, was bei der Vielzahl von Kunden großer Anbieter wie z. B. Amazon und Facebook schlicht unrealistisch wäre.

AGB werden von dem Unternehmen, das beispielsweise einen Dienst über das Internet anbietet, vorformuliert. Der Verbraucher muss die AGB i. d. R. im Rahmen der Erstanmeldung/-registrierung bei dem Online-Dienst bestätigen, damit die Regelungsinhalte der AGB für die Nutzung des Dienstes zwischen Anbieter und Verbraucher gelten.[1] Der Verbraucher kann i. d. R. keinen Einfluss auf die Inhalte der AGB nehmen. Auch wenn er mit einer oder mehreren Klauseln nicht einverstanden ist, hat er i. d. R. lediglich die Wahl, den Dienst zu den in den AGB stehenden Bedingungen zu nutzen oder sich einen alternativen Dienst/Anbieter zu suchen. Allein schon deswegen ist das Unternehmen, das die AGB vorformuliert und in das Vertragsverhältnis mit dem Verbraucher einbeziehen möchte, im Vergleich zum Verbraucher in einer stärkeren Position („Friss oder stirb“). Aber auch weil das Unternehmen i. d. R. über die personellen und finanziellen Ressourcen verfügt, um einen Streitfall vor Gericht auszutragen, während ein (potenzieller) Rechtsstreit gegen ein großes Unternehmen aus Sicht des Verbrauchers mit einem hohen finanziellen Risiko verbunden ist, sollen Verbraucher vor unverhältnismäßigen Nachteilen durch die anbieterseitig vorformulierten AGB geschützt werden. Aus diesem Grund enthält das Bürgerliche Gesetzbuch (BGB) in den §§ 305 ff. Regelungen zur wirksamen Einbeziehung und zur Wirksamkeit der AGB-Klauseln, um den Verbraucher u. a. vor „überraschenden Klauseln“ zu schützen.

Das folgende Kapitel zeigt an den beispielhaft ausgewählten Anbietern von PayPal, Microsoft Skype, Apple iTunes, Amazon Kindle, Sony PlayStation und Facebook auf, ob und welche der Anbieter in ihren AGB explizite Regelungen zur Vererbbarkeit digitaler Werte vorsehen und bewertet die Rechtskonformität dieser Regelungen. Auch sollen mögliche Benachteiligungen von Verbrauchern in Bezug auf das digitale Erbe bei der Dienstnutzung thematisiert werden und diskutiert werden, ob den Verbrauchern z. B. weitere Informationstexte zum digitalen Vererben im Rahmen der Dienstnutzung zur Verfügung stehen sollten und/oder etwa Anpassungen des Verbraucherschutzrechts erforderlich wären.

[1] Anders verhält es sich z. B. in Ladengeschäften, in denen der Hinweis auf die Einbeziehung der AGB bei Vertragsschluss regelmäßig mit unverhältnismäßigen Schwierigkeiten verbunden wäre. In diesen Fällen genügt i. d. R. ein gut sichtbarer Aushang der AGB am Ort des Vertragsschlusses, also i. d. R. an den Kassen des Ladengeschäfts.

5.2 Wichtige AGB von Anbietern digitaler Werte im Überblick

Das nachstehende Unterkapitel stellt zunächst überblicksartig die wichtigsten AGB-Klauseln zum digitalen Nachlass von PayPal, Microsoft Skype, Apple iTunes, Amazon Kindle, Sony PlayStation sowie Facebook dar. Obwohl man nur bei wenigen Anbietern explizite AGB-Klauseln für den Todesfall eines Nutzers findet, finden sich doch bei allen der untersuchten Anbieter zumindest AGB-Klauseln, die sich potenziell auf einen digitalen Nachlass auswirken können. Die dargestellten Klauseln bilden die Grundlage für die sich an das Unterkapitel anschließende Untersuchung der Rechte an digitalen Inhalten und der Rechtskonformität von AGB-Klauseln zum digitalen Nachlass. Sofern relevant, stellt das Unterkapitel zusätzlich weiterführende Informationen der Anbieter zum Thema des digitalen Nachlasses dar, die sich nicht in den AGB selbst, sondern beispielsweise in den Nutzerforen der Anbieter finden.

5.2.1 AGB von PayPal

PayPal ist ein Online-Bezahldienst, mit dessen Hilfe Nutzer im Internet schnell und sicher bezahlen können. Die Abrechnung erfolgt zwischen dem jeweiligen Onlineshop und PayPal, wobei der Nutzer in seinem PayPal-Account seine Bankverbindungsdaten angeben muss und/oder Geldwerte in seinem PayPal-Account verfügbar halten kann (z. B. durch Umbuchung eines Betrages von seinem Girokonto auf sein PayPal-Konto).

5.2.1.1 Regelungen in den AGB

In den AGB von PayPal sind keine expliziten Regelungen für den Todesfall des Kontoinhabers zu finden.[2] Sonstige relevante Regelungen in den AGB umfassen u. a. die Übertragung des Kontos und die Kontoschließung durch PayPal, siehe nachfolgende Unterabschnitte.

Übertragung des Kontos Eine Übertragung des Kontos an Dritte wird dem Kontoinhaber nicht gestattet. Auch darf der Kontoinhaber „keinerlei Rechte oder Verpflichtungen aus diesen Nutzungsbedingungen ohne die vorherige schriftliche Zustimmung von PayPal übertragen oder abtreten.“[3]

Kontoschließung durch PayPal Das PayPal-Konto kann fristlos geschlossen werden, wenn sich der Kontoinhaber für einen Zeitraum von drei Jahren nicht eingeloggt hat. Der Kontoinhaber wird über die Entscheidung informiert, um z. B. noch unbestrittenes Guthaben abbuchen zu können.[4]

[2] Dies gilt für die bis zum 18.08.2019 gültige Fassung als auch für die ab dem 19.08.2019 gültige neue Fassung. Siehe https://www.paypal.com/de/webapps/mpp/ua/useragreement-full#r1.

[3] Siehe neue Fassung der AGB 1.3. „Abtretung“, https://www.paypal.com/de/webapps/mpp/ua/useragreement-full#r1. Die folgenden Ausführungen beziehen sich auch auf die ab 19.08.2019 gültige Fassung.

[4] Siehe AGB 7.2 „Schließung des Kontos“, https://www.paypal.com/de/webapps/mpp/ua/useragreement-full#r1.

Mitteilungen an PayPal Mitteilungen an PayPal, die die Nutzungsbedingungen betreffen, sind per Brief an die in den AGB genannte Adresse der Rechtsabteilung am Hauptsitz des Unternehmens zu schicken.[5]

5.2.1.2 Hinweise außerhalb der AGB

Vermutlich denken nicht alle Erben in der Ausnahmesituation eines Todesfalls daran, die AGB eines Vertragspartners des Erblassers zu lesen. Dies kann man jedenfalls daraus schließen, dass manche Erben ihre Fragen im sogenannten „PayPal-Community-Hilfe Forum“ stellen, anstatt sie an die o. g. Rechtsabteilung zu richten. So hat z. B. eine Nutzerin (am 24.03.2018) gefragt, wie man eventuell noch vorhandenes Guthaben vom Konto ihres unerwartet verstorbenen Lebensgefährten zurückfordern und dann das Konto löschen lassen könne. Laut Antwort einer Moderatorin verlangt PayPal folgende Informationen und Dokumente:

- „Eine Erklärung, dass der Kontoinhaber verstorben ist, und dass der Erbe oder der Nachlassverwalter die Schließung des PayPal-Kontos wünscht.
- Eine Kopie der Sterbeurkunde des Kontoinhabers.
- Eine Kopie des Testaments des verstorbenen Kontoinhabers oder anderer rechtskräftiger Unterlagen, z. B. des Erbscheins. In dem Dokument müssen Name und Adresse des Erben oder des Nachlassverwalters stehen.
- Die Kopie der Vorder- und Rückseite des Personalausweises oder Reisepasses des Erben oder Nachlassverwalters.“

Außerdem wird noch darauf hingewiesen, dass eine Gebühr von 40 US-Dollar bzw. der entsprechenden Summe in Euro fällig werde, wenn ein zurückzuerstattendes Guthaben nicht auf ein anderes PayPal-Konto bzw. das im PayPal-Konto des Erblassers registrierte Bankkonto überwiesen werden soll. Diese Antwort steht auch als Musterlösung unter ähnlichen Anfragen, wobei zwei weitere Nutzer darauf hinweisen, dass die Übermittlung der geforderten Unterlagen über die in der Antwort enthaltene Faxnummer nicht funktioniere.[6]

5.2.2 AGB von Microsoft Skype

Skype ist ein Instant-Messaging-Dienst, der es seinen Nutzern u.a. erlaubt, unter Nutzung einer speziellen Software kostenlose Telefonate, Chats und Videokonferenzen zu führen. Skype bietet neben kostenlosen Angeboten auch kostenpflichtige Angebote an, für die die Nutzer Skype-Guthaben erwerben können (i. d R. durch Bezahlung über PayPal oder per Kreditkarte), wobei die Nutzung des Skype-Guthabens vergleichbar mit der früher in Telefonzellen eingesetzten Telefonkarte ist.

[5] Siehe AGB, 1.5

[6] Die erwähnten Fragen und die Antwort sind zu finden unter https://www.paypal-community.com/t5/Kontosicherheit/Paypal-Konto-eines-verstorbenen-löschen/m-p/1493288/highlight/true#M3283.

5.2.2.1 Regelungen in den AGB

Die Nutzungsbedingungen von Skype (Stand 01.06.2018) enthalten keine speziellen Regelungen für den Todesfall. Sonstige relevante Regelungen in den AGB umfassen:

Übertragung des Kontos Für die Nutzung von Microsoft-Diensten wie Skype ist ein Microsoft-Konto einzurichten. Laut dem „Microsoft-Servicevertrag“ darf der Kunde „die Anmeldeinformationen für sein Microsoft-Konto nicht an einen anderen Nutzer oder eine andere juristische Person übertragen“ und hat die Kontodetails und das Kennwort zum Schutz des Kontos vertraulich zu behandeln.[7]

Softwarelizenz Privatkunden wird eine „beschränkte, nicht exklusive, nicht unterlizenzierbare, nicht übertragbare, kostenlose Lizenz für das Herunterladen und Installieren der Software auf einem PC, einem Handy oder einem anderen Gerät gewährt.“ Des Weiteren darf der Kunde die Software über das individuelle Nutzerkonto persönlich nutzen.[8]

Skype-Guthaben Zu Skype-Guthaben, das vom Kunden vorab gekauft wurde, um z. B. via Skype ins Mobilfunknetz zu telefonieren oder SMS zu senden, heißt es in den Skype-Nutzungsbedingungen: „Falls Sie Skype-Guthaben kaufen, sollten Sie sich der Tatsache bewusst sein, dass es inaktiv wird, wenn Sie es 180 Tage nicht genutzt haben.“ Es ist laut AGB zwar möglich, inaktives Guthaben wieder zu aktivieren, aber mit der Einschränkung, das wieder aktiviertes Guthaben nicht rückerstattungsfähig ist.[9]

5.2.2.2 Hinweise außerhalb der AGB

Über das Suchfeld in der Microsoft-Community[10] findet man die Frage einer Nutzerin, die nach dem Todesfall ihres Vaters eine Abbuchung rückgängig machen und das Konto schließen möchte. Eine Microsoft-Moderatorin antwortet, dass Skype-Kontos von Verstorbenen über den Microsoft-Support gelöscht werden. Wegen der Rückgängigmachung der Abbuchung solle die Tochter sich an den Skype-Support wenden. Die Antwort enthält die jeweiligen Internet-Links zu den zwei Supports.[11]

[7] Siehe https://www.microsoft.com/de-de/servicesagreement 4.a.i. „Erstellung eines Kontos“.
[8] Siehe „Skype-Nutzungsbedingungen, 4.1 Lizenz“ https://www.skype.com/de/legal/ios/tos/#14.
[9] Siehe „Wichtigste Punkte, Skype-Guthaben“ und Klausel 9.2 „Inaktives Skype-Guthaben“ https://www.skype.com/de/legal/ios/tos/#14.
[10] Siehe https://answers.microsoft.com/de-de.
[11] Siehe o. g. Antwort vom 12.09.2017 https://answers.microsoft.com/de-de.

5.2.3 AGB von Apple iTunes

iTunes ist eine Medienverwaltungssoftware, mit der man etwa Musik, Filme, TV-Serien, Podcasts und Hörbücher verwalten, abspielen und durch Synchronisation auf weitere Apple-Geräte übertragen kann. Vorgenannte Medien werden im iTunes Store (kostenpflichtig, teilweise auch kostenlos) angeboten, auf den man direkt über iTunes zugreifen kann. Ebenso kann man auf Appple-Dienste zugreifen, die man kostenpflichtig abonnieren kann, etwa den Musikstreaming-Dienst „Apple Music“.

Die „Bedingungen der Apple Media Services“ enthalten keine Regelungen für den Todesfall.[12]

5.2.3.1 (Kein) Recht des Überlebenden

In den AGB zu einem weiteren Dienst von Apple, der iCloud, ist unter der Überschrift „Kein Recht des Überlebenden“ folgende Klausel zu lesen: „Sofern gesetzlich nichts anderes vorgeschrieben ist, stimmst du zu, dass dein Account nicht übertragbar ist und dass alle Rechte an deiner Apple-ID oder deinen Inhalten innerhalb deines Accounts im Falle deines Todes enden. Bei Erhalt einer Kopie deiner Sterbeurkunde können dein Account aufgelöst und sämtliche Inhalte innerhalb deines Accounts gelöscht werden.“ Die Klausel enthält weiterhin einen Internet-Link zum iCloud-Support, an den sich der Kunde wenden könne, wenn er weitere Unterstützung wünsche.[13] Sonstige relevante Regelungen in den AGB umfassen:

5.2.3.2 Kundenkonto

Zur Nutzung der Apple-Dienste ist die Einrichtung eines Kontos mit einer sogenannten Apple-ID erforderlich. Darüber kann der Kunde Inhalte wie Applikationen („Apps“) und sonstige In-App-Dienste erwerben bzw. gemäß dem AGB-Wortlaut „kaufen, beziehen, lizenzieren, mieten oder abonnieren“. Inhalte können neben Apple[14] auch von Drittanbietern angeboten werden.[15]

5.2.3.3 Lizenz: Allgemeine Regelungen

Unter dem Punkt „Zahlungen, Steuern und Erstattungen“ der AGB wird erklärt, dass der Kunde für jede sogenannte Transaktion, d. h. kostenlose oder kostenpflichtige Inhalte, die er über die Apple-Dienste erwirbt, lediglich eine Lizenz zur Nutzung erhält. Auch wenn Apple der Vertragspartner für

[12] Bedingungen der Apple Media Services, Abschnitte A., B., Stand 13.05.2019, abrufbar unter https://www.apple.com/legal/internet-services/itunes/de/terms.html.

[13] iCloud Nutzungsbedingungen, Abschnitt IV. D., Stand 17. September 2018, abrufbar unter https://www.apple.com/de/legal/internet-services/icloud/de/terms.html.

[14] Vertragspartner für Deutschland ist „Apple Distribution International“ mit Sitz in Irland. Kontaktdaten sind abrufbar unter https://www.apple.com/de/contact.

[15] Bedingungen der Apple Media Services, Abschnitte A., B., Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html.

die Inhalte ist, können Dritte die Lizenzgeber sein. Beispielsweise können Apps von Apple oder von Drittentwicklern, den sogenannten App-Providern, und Bücher von Buchverlegern lizenziert sein.[16]

Dass die Nutzungslizenz für gekaufte Inhalte – im Gegensatz zu gemieteten Inhalten, die nur befristet zur Verfügung stehen – zeitlich unbegrenzt ist (bzw. sein sollte), wird in den AGB nicht direkt erwähnt. Indirekt kann man dies aus der Empfehlung ableiten, von heruntergeladenen Inhalten regelmäßig Sicherungskopien zu erstellen.[17]

5.2.3.4 Gekaufte und gemietete Audio- und Video-Inhalte

Unterschieden zwischen Kauf und Miete wird auch im Abschnitt „Gekaufte und gemietete Audio- und Video-Inhalte." Dort erfährt der Kunde u. a., dass gemietete Inhalte innerhalb von 30 Tagen abgespielt werden müssen.

Für Playlists gekaufter Musik ist es laut AGB erlaubt, diese bis zu siebenmal zu brennen (die quantitative Begrenzung gilt nicht für DRM-freie Inhalte). Andere Inhalte dürfen nicht gebrannt werden.[18]

5.2.3.5 Von Nutzern generierte Beiträge

Soweit Dienste eigene Beiträge wie etwa Kommentare, Bilder, Videos, Podcasts erlauben, räumt der Kunde Apple eine weltweite, kostenlose, unbefristete und nicht-exklusive Lizenz zu deren Nutzung und Vermarktung sowie zu internen Zwecken von Apple ein. Der Zweck der Lizenz ist begrenzt auf den Betrieb der Dienste.

5.2.4 AGB von Amazon Kindle

Bei Amazon Kindle handelt es sich um eine Produktserie von sogenannten e-Book-Readern, also kleinen Tabletcomputern mit einem besonders kontrastreichen Bildschirm, auf dem die Nutzer elektronische Bücher und Zeitschriften lesen können. Die Bücher und Zeitschriften können direkt bei Amazon erworben und auf das Endgerät geladen werden.

Es gibt keine spezifischen Regelungen für den Todesfall eines Kontoinhabers. Sonstige Regelungen in den AGB umfassen u. a. das Kundenkonto und die Nutzungsbedingungen für den Kindle-Shop.

[16] Bedingungen der Apple Media Services, Abschnitt B., Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html.

[17] Bedingungen der Apple Media Services, Abschnitt B., „Regeln für die Nutzung der Dienste und Inhalte", Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html; Anleitung „iTunes-Mediathek sichern und wiederherstellen", https://support.apple.com/de-de/HT201625.

[18] Bedingungen der Apple Media Services, Abschnitt B., „Regeln für die Nutzung der Dienste und Inhalte", Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html.

5.2.4.1 Kundenkonto

Bezüglich Amazon Kindle gibt es verschiedene Nutzungsbedingungen, was zumindest verwirrend für den Kunden bzw. seinen Erben sein dürfte. U. a. sind auf Amazon.de[19] folgende Dokumente zu finden: „Nutzungsbedingungen für Kindle eReader und Fire Tablets“, „Lizenzvereinbarung und Nutzungsbedingungen für Amazon.de Kindle“, „Nutzungsbedingungen für den Kindle-Shop“. Des Weiteren wird innerhalb der vorgenannten Bedingungen auf weitere Regelungen verwiesen, z. B. auf die „Amazon.de Allgemeinen Geschäftsbedingungen“, die u. a. allgemeine Regelungen zum E-Commerce und dem Kundenkonto beinhalten.

Das Kundenkonto wird für die Nutzung vieler Services benötigt.[20] Nach den Informationen im Bereich „Hilfe und Kundenservice“ muss der Kunde den Kindle eReader in seinem Amazon-Konto anmelden, „um Kindle-Inhalte kaufen und senden zu können“.[21]

5.2.4.2 Nutzungsbedingungen für den Kindle-Shop

In vorgenannten Nutzungsbedingungen,[22] die der Kunde – neben diversen weiteren Bedingungen – laut den „Nutzungsbedingungen für Kindle eReader und Fire Tablets“ z. B. mit der Bestellung oder der Registrierung eines Kindle eReaders anerkennt, wird der Kunde unter dem Punkt „1. Kindle-Inhalte“ darauf hingewiesen, dass ihm der Anbieter von Inhalten (neben Amazon auch Drittanbieter) ein nicht-exklusives Recht gewährt, die Kindle-Inhalte ausschließlich für die persönliche, private Nutzung unbegrenzt, nur auf so vielen Geräten, wie dies im Kindle-Shop angegeben wurde anzusehen, zu nutzen und anzuzeigen. Weiterhin wird dem Kunden erklärt: „Ihre Kindle-Inhalte werden durch den Anbieter von Inhalten lizenziert, nicht aber verkauft. Der Anbieter von Inhalten kann weitere Nutzungsbedingungen in die Kindle-Inhalte aufnehmen ...“ Wie oben erwähnt, wird aber im Bereich „Hilfe und Kundenservice“ der Begriff „kaufen“ verwendet.

Die Nutzungsbedingungen enthalten die Beschränkung, dass der Kunde die Rechte an den Kindle-Inhalten oder Teilen davon nicht verkaufen, vermieten, verleihen, vertreiben, im Rundfunk ausstrahlen, unterlizenzieren oder anderweitig an Dritte abtreten darf, sofern nichts anderes ausdrücklich angegeben ist.

Unter „2. Nutzung der Kindle-Anwendungen“ ist wiederum ein Verweis auf die „Amazon.de Allgemeinen Geschäftsbedingungen“, die entsprechende und weitere Lizenzbedingungen enthalten.

[19] Die Links zu den o. g. Dokumenten sind abrufbar unter https://www.amazon.de/gp/help/customer/display.html?nodeId=200144520.

[20] „Amazon.de Allgemeinen Geschäftsbedingungen“, https://www.amazon.de/gp/help/customer/display.html?&nodeId=505048.

[21] „Amazon Hilfe und Kundenservice“, https://www.amazon.de/gp/help/customer/display.html?nodeId=201733370.

[22] Nutzungsbedingungen für den Kindle-Shop, abrufbar unter https://www.amazon.de/gp/help/customer/display.html?nodeId=201014950.

5.2.5 AGB von Sony PlayStation

Bei einer PlayStation handelt es sich um eine Spielekonsole. PlayStation bietet ihren Nutzern die Möglichkeit, Guthaben für den PlayStation Store zu erwerben. Im PlayStation Store können wiederum u. a. Spiele und Spielerweiterungen gekauft werden, um diese über die PlayStation zu nutzen.

Es gibt keine spezifischen Regelungen für den Todesfall eines Kontoinhabers. Sonstige Regelungen in den AGB umfassen:

5.2.5.1 AGB für das PlayStation Network (PSN)

Kundenkonto

Über das Konto erhält der Kunde Zugriff auf diverse kostenlose und kostenpflichtige Online-Services und digitale Inhalte, etwa „PSN“, „PlayStation Store“ (angeboten werden Spiele, Online-Spiele, Musik, Filme, Abonnements), Online-Guthaben, virtuelle Communities (für Kommunikation und gemeinsames Spielen), die zusammenfassend als Produkte bezeichnet werden.[23] Unter 18-Jährige dürfen ein Konto mit PSN-Zugang nur dann besitzen, wenn ein Elternteil oder Erziehungsberechtigter bei der Kontoerstellung geholfen und sich damit einverstanden erklärt hat (das Mindestalter beträgt 7 Jahre).[24]

Auflösen des Kontos

Wird das Konto mindestens 24 Monate nicht mehr verwendet, kann Sony es auflösen. Auch der Kunde kann das Konto auflösen, indem er sich an eine in den AGB genannte Adresse wendet. In beiden Fällen wird ungenutztes Guthaben oder noch nicht abgelaufene Teile eines Abonnements nicht zurückerstattet, mit der Einschränkung „sofern wir nicht gesetzlich dazu verpflichtet sind“.[25]

Hinzufügen von PSN-Guthaben und Geld

Das Konto kann (durch unterschiedliche Zahlungsmethoden) mit zugehörigem PSN-Guthaben aufgeladen werden, wenn der Kunde sich in einem Land befindet, das einen PlayStation Store besitzt.[26] Rückerstattungen sind laut den AGB bis auf folgende Ausnahmen ausgeschlossen: Wenn das Konto infolge einer Änderung der PSN-Nutzungsbedingungen oder der Softwarenutzungsbedingungen, die der Kunde nicht akzeptiert, geschlossen wird oder wenn es gesetzlich erforderlich ist.[27]

[23] PSN Nutzungsbedingungen,(i), Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.
[24] PSN Nutzungsbedingungen,(i), Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.
[25] PSN Nutzungsbedingungen, 17., Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.
[26] Ob ein PlayStation Store bzw. welche anderen Services angeboten werden, ist abrufbar unter https://status.playstation.com/de-de.
[27] PSN Nutzungsbedingungen, 6. (i), (xii), Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

Keine Guthaben-Übertragung oder Umtausch in Bargeld

Das Guthaben kann laut den AGB nicht auf andere übertragen werden. Außerdem wird erklärt: „PSN-Guthaben besitzen keinen Wert außerhalb des PSN, können nur zum Kauf der von uns angebotenen Produkte genutzt werden, können nicht in Bargeld eingelöst werden, sind nicht Ihr persönliches Eigentum [...].“[28]

Mindestbetrag und befristete Gültigkeit des PSN-Guthabens

Sony kann einen Mindestbetrag für die Aufstockung des PSN-Guthabens festlegen. Das PSN-Guthaben muss innerhalb von 24 Monaten verwendet werden.[29]

Lizenz

Im Abschnitt „Erwerb von Produkten“ enthalten die AGB u. a. folgende Klausel für PlayStation Video: „Gemäß Abschnitt 12 stehen Ihnen die erworbenen Produkte eine angemessene Zeit lang als Download oder Stream (sofern anwendbar) zur Verfügung.“ Weiterhin wird mit Verweis auf den Abschnitt „Rechte an geistigem Eigentum (einschließlich unrechtmäßig hergestellter Software)“ erklärt: Sie erwerben eine Lizenz zur Nutzung der Produkte – siehe Abschnitt 13. Über diese Lizenz hinaus haben Sie keinerlei Eigentums-, Besitz-, ökonomische oder finanzielle Ansprüche an Produkten, die Sie erwerben.“[30] Im o. g. Abschnitt zum geistigen Eigentum wird u. a. erläutert, dass der Kunde beim Erwerb von Produkten (ausgenommen Software, für die gesonderte Nutzungsbedingungen bestehen, s. u.) eine begrenzte, nicht exklusive, nicht übertragbare und persönliche Lizenz zur Nutzung erhält.

Nutzergenerierte Medien (UGM)

Nutzt der Kunde die Community-Funktionen des PSN, kann er Texte, Nachrichten, Kommentare, Bilder, Fotoaufnahmen, Videos, Spielinhalte, Spielvideos oder andere Materialien und Informationen teilen (sogenannte „User Generated Media“ UGM).[31]

Beanspruchung der Rechte an UGM Ohne zu unterscheiden, ob UGM auf geistigem Eigentum des Anbieters basiert (etwa die Bearbeitung des Screenshots eines Spiels) oder nicht, soll der Kunde auf nahezu alle Rechte daran verzichten: „UGM, die von Ihnen erstellt und geteilt wurden, gehören zwar Ihnen, aber wir und, sofern geltend, der entsprechende Produkt-Herausgeber behalten uns das Recht auf dieses geistige Eigentum vor. Es ist daher untersagt, UGM für kommerzielle Zwecke zu nutzen, ohne dass hierfür unsere Zustimmung oder die des Produkt-Herausgebers vorliegt.“ So

[28] PSN Nutzungsbedingungen, 6. (xi), Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

[29] PSN Nutzungsbedingungen, 6. (iv), (ix), Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

[30] PSN Nutzungsbedingungen, 7. (vii),(viii) Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

[31] PSN-Nutzungsbedingungen, 13., Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

autorisiert der Kunde laut den AGB Sony, verbundene Unternehmen sowie andere PSN-Nutzer zur Verbreitung, Kopie, Modifizierung und Veröffentlichung der UGM und seiner Online-ID in PSN und anderen mit PlayStation verbundenen Diensten. Ohne Gegenleistung räumt Sony sich und verbunden Unternehmen die Rechte ein, UGM zu lizenzieren, zu verkaufen oder auf sonstige Art und Weise kommerziell zu verwenden (etwa durch das Verkaufen von Zugriff auf die UGM bzw. für Werbung.) Auch soll der Kunde auf eventuelle Persönlichkeitsrechte verzichten.[32]

Softwarenutzungsbedingungen

Die AGB für das PSN verweisen auf weitere AGB, z. B. die Softwarenutzungsbedingungen. Diese sind wiederum nach den Geräten, die der Kunde nutzt, getrennt. Es bestehen AGB für die PS-Spielekonsolen und AGB für PC und Mobilgeräte. Die nachfolgend erwähnten Regelungen sind in beiden Versionen enthalten.[33] Zusätzlich können weitere Nutzungsbedingungen zu beachten sein, wenn es sich um Software von Drittanbietern handelt.

Lizenz Dem Kunden wird erklärt, dass er die Software gemäß den Bedingungen nutzen darf, jedoch kein Eigentümer der Software ist.[34]

Einschränkungen Die Lizenz ist nicht-exklusiv und nicht-übertragbar, berechtigt nur zur privaten Nutzung der Software und nur in Europa, dem Nahen Osten, Afrika, Indien, Russland und Ozeanien. Verboten sind u. a. kommerzielle Nutzung, Verbreitung und Weiterverkauf (ohne ausdrückliche Erlaubnis).[35]

5.2.6 AGB von Facebook

Bei Facebook handelt es sich um ein soziales Netzwerk. Facebook erlaubt es seinen Nutzern, mit Freunden und Verwandten auf der ganzen Welt auf einfach Weise in Kontakt zu bleiben. Über Beiträge, die der Nutzer in seinem Profil veröffentlicht, kann er mit seinen Facebook-Kontakten u. a. Urlaubsbilder teilen und über ein für ihn wichtiges Ereignis informieren. Auch können Nutzer untereinander private Nachrichten austauschen.

[32] PSN Nutzungsbedingungen, 13., Stand Oktober 2017, https://legaldoc.dl.playstation.net/ps3-eula/psn/e/e_tosua_de.html.

[33] Softwarenutzungsbedingungen der für die Spielekonsolen, Stand Oktober 2017, https://www.playstation.com/de-de/legal/software-usage-terms. Softwarenutzungsbedingungen für PC und Mobilgeräte, Stand Oktober 2015, https://www.playstation.com/de-de/legal/application-terms-of-use-for-pc-and-mobile.

[34] Softwarenutzungsbedingungen für Konsolen bzw. für PC und Mobilgeräte, jeweils Abschnitt 4.

[35] Softwarenutzungsbedingungen für Konsolen, Abschnitt 6 bzw. für PC und Mobilgeräte Abschnitte 5 und 6.

5.2.6.1 Regelungen in den AGB

Nachlasskontakt

Unter „Sonstiges“ der AGB[36] ist folgende Regelung zu finden: „Du kannst eine Person benennen (den sogenannte Nachlasskontakt), die dein Konto verwaltet, wenn es in den Gedenkzustand versetzt wird. Nur dein Nachlasskontakt oder eine Person, die du in einem gültigen Testament oder ähnlichen Dokument, das deine eindeutige Zustimmung zur Offenlegung deiner Inhalte im Todesfall oder bei Unfähigkeit ausdrückt, genannt hast, kann die Offenlegung deines Kontos beantragen, nachdem es in den Gedenkzustand versetzt worden ist.“[37]

Sonstige Regelungen in den AGB umfassen:

Auschluss der Übertragbarkeit des Accounts

Der Nutzer darf sein Konto laut den AGB „nicht an jemand anderen übertragen (ohne unsere Genehmigung)“. Dieselbe Klausel enthält noch die Vorgaben, dass der Nutzer sein Passwort nicht weitergeben und anderen keinen Zugriff auf sein Facebook-Konto gewähren darf.[38]

Rechte von Facebook an den von Nutzern eingestellten Inhalten

Facebook gewährt sich weitgehende Nutzungsbedingungen bezüglich der Inhalte der Nutzer:

> „... insbesondere wenn du Inhalte, die durch geistige Eigentumsrechte geschützt sind (wie Fotos oder Videos), auf oder in Verbindung mit unseren Produkten teilst, postest oder hochlädst, gewährst du uns eine nicht-exklusive, übertragbare, unterlizenzierbare und weltweite Lizenz, deine Inhalte (gemäß deinen Privatsphäre- und App-Einstellungen) zu hosten, zu verwenden, zu verbreiten, zu modifizieren, auszuführen, zu kopieren, öffentlich vorzuführen oder anzuzeigen, zu übersetzen und abgeleitete Werke davon zu erstellen. Diese Lizenz dient nur dem Zweck, dir unsere Produkte bereitzustellen. Das bedeutet beispielsweise, dass du uns, wenn du ein Foto auf Facebook teilst, die Berechtigung gibst, es zu speichern, zu kopieren und mit anderen zu teilen (wiederum im Einklang mit deinen Einstellungen); dies können u. a. Dienstleister sein, die unseren Dienst oder andere von dir genutzte Facebook-Produkte unterstützen.

[36] Die Bewertung der Nutzungsbedingungen in diesem Abschnitt bezieht sich auf die Version der Facebook-Nutzungsbedingungen vom 19.04.2018. Die Nutzungsbedingungen von Facebook wurden während der Bearbeitungszeit der Studie (am 31.07.2019) geändert. Gleich geblieben sind aber die Regelung zum Nachlasskontakt und der Ausschluss der Übertragbarkeit des Kontos (zu Lebzeiten) an Dritte in den AGB selbst, sodass die Ausführungen dieses Kapitels zu den AGB nach wie vor als aktuell anzusehen sind. Auch eine stichprobenartige Prüfung des Hilfebereichs ergab keine Änderung hinsichtlich der Befugnisse des Nachlasskontakts. Dieser kann nach wie vor die Löschung des Kontos veranlassen, soweit der Nutzer/Erblasser dies vorher festgelegt hat.

[37] Nutzungsbedingungen Facebook, Abschnitt 4. Punkt 5., Stand 19.04.2018, https://de-de.facebook.com/legal/terms?ref=pf, zuletzt abgerufen am 27.06.2019.

[38] Nutzungsbedingungen Facebook, Abschnitt 3. Punkt 1., Stand 19.04.2018, https://de-de.facebook.com/legal/terms?ref=pf.

> Du kannst diese Lizenz jederzeit beenden, indem du deine Inhalte oder dein Konto löschst. Du solltest wissen, dass aus technischen Gründen von dir gelöschte Inhalte möglicherweise für einen begrenzten Zeitraum in Sicherheitskopien bestehen bleiben. (Sie sind dann jedoch nicht mehr für andere Nutzer/innen sichtbar). Darüber hinaus erscheinen von dir gelöschte Inhalte möglicherweise weiterhin, wenn du diese mit anderen geteilt hast und diese Personen sie nicht gelöscht haben.
>
> Verwendung deines Namens, deines Profilbildes sowie von Informationen über deine Interaktionen mit Werbeanzeigen und gesponserten Inhalten: Dein Name und dein Profilbild sowie Informationen über Handlungen, die du auf Facebook vorgenommen hast, können neben oder in Verbindung mit Werbeanzeigen, Angeboten und sonstigen gesponserten Inhalten verwendet werden, die wir in unseren Produkten anzeigen, ohne dass du hierfür einen Ausgleich erhältst. Beispielsweise können wir deinen Freunden anzeigen, dass du an einer beworbenen Veranstaltung interessiert bist oder eine Seite mit „Gefällt mir" markiert hast, die von einer Marke erstellt worden ist, die uns dafür bezahlt hat, dass wir ihre Werbeanzeigen auf Facebook zeigen. Werbeanzeigen wie diese können nur von Personen gesehen werden, die deine Erlaubnis haben, die von dir auf Facebook vorgenommenen Handlungen zu sehen. Erfahre mehr zu deinen Einstellungen für Werbeanzeigen und deinen Werbepräferenzen."[39]

5.2.6.2 Hinweise außerhalb der AGB

Besondere Anfrage für Konto eines Verstorbenen

Im Hilfebereich stellt Facebook das Kontaktformular „Besondere Anfrage für ein Konto einer medizinisch stark beeinträchtigten oder verstorbenen Person" bereit,[40] mit dem man entsprechende Konten entfernen oder in den Gedenkzustand versetzen lassen kann. Außerdem teilt Facebook mit, zum Schutz der Privatsphäre von Facebook-Nutzern keine Anmeldedaten für Konten freigeben zu können. Um das Konto zu entfernen oder besonderen Anfragen nachkommen zu können, benötigt Facebook einen Nachweis, dass man ein direktes Familienmitglied oder Nachlassverwalter ist.

Folgende Angaben werden in o. g. Kontaktformular abgefragt: Vollständiger Name und E-Mail-Adresse des Anfragenden, Profilname, Link (URL) zum Profil, E-Mail-Adresse des Kontoinhabers.

Möchte der Anfragende das Konto in den Gedenkzustand versetzen lassen, benötigt Facebook zur Bestätigung des Sterbefalls einen Scan oder ein Foto der Todesanzeige, der Sterbeurkunde, der Trauerkarte oder eines anderen Dokuments des/der Verstorbenen.

[39] Da diese Klausel gemäß dem Facebook-Urteil des BGH keinen Einfluss auf die Vererbarkeit der Inhalte hat, da sich kein höchstpersönliches Vertragsverhältnis daraus ergebe, dass die Nutzer Facebook die „nicht-exklusive, übertragbare, unterlizensierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte" gewähren, wurden entsprechende Klauseln der Anbieter nachstehend nicht geprüft. *BGH*, NJW 2018, S. 3178 (3183) Rn. 51.

[40] Facebook-Hilfethema „Besondere Anfrage für ein Konto einer medizinisch stark beeinträchtigten oder verstorbenen Person", https://de-de.facebook.com/help/contact/228813257197480.

Geht es um die Entfernung des Kontos und kann der Anfragende keine Sterbeurkunde vorlegen, akzeptiert Facebook auch die Todesanzeige oder Trauerkarte, wenn der Anfragende zusätzlich einen Berechtigungsnachweis vorlegen kann (z. B. Vollmacht, Geburtsurkunde, Testament, Nachlassbrief).[41] Am Ende des Kontaktformulars befindet sich folgende Einschränkung, die dem Nachlasskontakt Vorrang gegenüber Erben einzuräumen scheint: „Folgendes ist zu beachten, wenn für das Konto ein Nachlasskontakt eingerichtet ist: Nur der Nachlasskontakt kann einen Antrag stellen, um das Profil entfernen zu lassen. Das Profil kann in den Gedenkzustand versetzt werden und verbleibt in diesem Gedenkzustand, es sei denn, der Nachlasskontakt stellt einen Antrag, um das Profil entfernen zu lassen."

Inhalte verstorbener Nutzer

Auch unter dem Hilfe-Thema: „Wie kann ich Inhalte des Facebook-Kontos eines verstorbenen Nutzers anfordern?", geht Facebook nicht auf eventuelle rechtliche Verpflichtungen zur Zugänglichmachung zu Inhalten von Verstorbenen ein: „In seltenen Fällen berücksichtigen wir Anfragen zu weiteren Kontoinformationen oder -inhalten. Du bist verpflichtet, nachzuweisen, dass du ein autorisierter Vertreter bist (z. B. Familienmitglied) und über eine Vollmacht verfügst. Bitte beachte, dass das Senden einer Anfrage oder das Ausfüllen der entsprechenden Dokumentation nicht zwangsläufig bedeutet, dass wir dir die Kontoinhalte der verstorbenen Person tatsächlich zur Verfügung stellen können. Darüber hinaus versetzen wir das Konto der verstorbenen Person in den Gedenkzustand, sobald wir deine Anfrage erhalten haben."[42] Auf dieser Hilfeseite ist ein Link zu einem entsprechenden Kontaktformular. Neben weiteren Dokumenten wird dort die Kopie der Sterbeurkunde des Verstorbenen verlangt bzw. falls diese nicht in Englisch vorliegt eine beglaubigte Übersetzung, was mit Kosten für den Erben verbunden ist.[43]

Informationen für den Nutzer

Im Hilfebereich stehen unter „Was passiert nach meinem Tod mit meinem Facebook-Konto?" folgende Informationen: Der Nutzer kann entweder einen Nachlasskontakt bestimmen, der sich um das – dann in den Gedenkzustand versetzte – Konto kümmert, oder festlegen, dass sein Konto dauerhaft gelöscht wird. Sofern der Nutzer nicht die Löschung seines Kontos veranlasst hat, wird es in den Gedenkzustand versetzt, wenn Facebook über seinen Tod in Kenntnis gesetzt wird. Bezüglich Konten im Gedenkzustand zählt Facebook folgende Eigenschaften auf:

- „Im Profil der verstorbenen Person wird vor ihrem Namen In Erinnerung an angezeigt.
- Wenn es die Privatsphäre-Einstellungen des Kontos erlauben, können Freunde Erinnerungen in der Chronik im Gedenkzustand teilen.

[41] „Wie kann ich die Entfernung des Facebook-Kontos eines verstorbenen Familienangehörigen beantragen?", https://www.facebook.com/help/1518259735093203.

[42] Facebook-Hilfethema „Wie kann ich Inhalte des Facebook-Kontos eines verstorbenen Nutzers anfordern?", https://de-de.facebook.com/help/123355624495297?helpref=related&ref=related.

[43] Antrag auf Erhalt von Inhalten des Kontos einer verstorbenen Person", https://de-de.facebook.com/help/contact/398036060275245.

- Die von der Person geteilten Inhalte, z. B. Fotos oder Beiträge, bleiben auf Facebook für die Zielgruppe sichtbar, mit der sie geteilt wurden.
- Profile im Gedenkzustand erscheinen nicht öffentlich, etwa im Abschnitt „Personen, die du kennen könntest“, in Anzeigen oder Geburtstagserinnerungen.
- Niemand kann sich bei einem Konto im Gedenkzustand anmelden.
- Konten im Gedenkzustand ohne Nachlasskontakt können nicht geändert werden.
- Seiten mit nur einem Admin, dessen Konto in den Gedenkzustand versetzt wurde, werden von Facebook auf einen gültigen Antrag auf Herstellung des Gedenkzustands hin entfernt.“

Facebook empfiehlt dringend, einen Nachlasskontakt festzulegen, damit das Konto auch im Gedenkzustand verwaltet werden könne. Der Nutzer muss allerdings mindestens 18 Jahre alt sein, um einen Nachlasskontakt bestimmen zu können.[44]

In seinen „Nachlass“-Einstellungen kann der Nutzer dem Nachlasskontakt erlauben, von dem Konto im Gedenkzustand ein Archiv der geteilten Informationen herunterzuladen (Fotos, Videos, Pinnwand-Einträge, Profil- und Kontaktinformationen, Ereignisse und Freundesliste). Zugriff auf Informationen wie z. B. Nachrichten oder Fotos, die der Nutzer automatisch synchronisiert, aber nicht gepostet hat, gewährt Facebook „möglicherweise [...] wenn ein gültiges Testament oder eine andere wirksame Einwilligung mit einem eindeutigen Einverständnis vorliegt“.[45]

Als Nachlasskontakt kann nur ein Facebook-Freund eingesetzt werden.[46]

5.3 Rechte an digitalen Inhalten

Das nachfolgende Unterkapitel untersucht die Rechte an digitalen Inhalten. Die Untersuchung stellt eine grundlegende Voraussetzung für die Bewertung der Rechtskonformität von AGB-Klauseln zum digitalen Nachlass dar, die wiederum den Schwerpunkt des darauffolgenden Unterkapitels bildet.

5.3.1 Abgrenzung Speichermedien, digitale Daten, digitale Inhalte

Als Grundlage der Untersuchung sind zunächst Speichermedien, digitale Daten und digitale Inhalte voneinander abzugrenzen.

[44] Facebook-Hilfethema „Was sind Nachlasskontakte und was können sie mit meinem Facebook-Konto tun?“, https://de-de.facebook.com/help/1070665206293088?helpref=faq_content.

[45] Facebook-Hilfethema „Welche Daten kann ein Nachlasskontakt von Facebook herunterladen?“, https://de-de.facebook.com/help/408044339354739.

[46] Facebook-Hilfethema „Kann ich eine Person, die kein Facebook-Freund ist, als meinen Nachlasskontakt auswählen?“, https://www.facebook.com/help/1585126361706709.

5.3.1.1 Speichermedium

Wie unter Kapitel 2.2 auf Seite 36 bereits ausgeführt, handelt es sich bei lokalen Datenträgern oder Speichermedien des Erblassers (wie Festplatten, CD-Roms, USB-Sticks) um Sachen im Sinne des § 90 BGB, deren Eigentum samt ihrem gespeicherten Inhalt gemäß § 1922 I BGB auf die Erben übergeht.[47]

5.3.1.2 Speicherung in der Cloud

Bei Nutzung von online zugänglichem Speicherplatz, etwa dem Speichern der Daten in der Cloud, erlangt der Nutzer keine Eigentums- oder Besitzrechte an diesem Speicherplatz. Zwischen ihm und dem Anbieter besteht ein mietvertragliches Verhältnis, das keine Besitzverschaffung, sondern lediglich eine Gebrauchsüberlassung voraussetzt.[48,49] Der Nutzer hat aus diesem Vertragsverhältnis einen Anspruch gegen den Anbieter, dass seine Daten unverändert gespeichert werden und er sie abrufen, ändern oder löschen kann.[50,51]

5.3.1.3 Digitale Daten

Im Gegensatz zu Speichermedien besitzen digitale Daten als solche keine Sachqualität im Sinne des § 90 BGB. Sie können aber als Wirtschaftsgüter gehandelt werden und Gegenstand von Verträgen sein.[52] So können sie u. a. (wie beispielsweise auch elektrischer Strom) als „sonstige Gegenstände“ gemäß § 453 I Alt. 1 BGB verkauft werden, d. h. gegen Zahlung eines Entgelts dauerhaft überlassen werden. Werden die Daten auf einem Speichermedium verkörpert, können sie Sachqualität erlangen. Nach Rechtsprechung des BGH ist auf einem Datenträger verkörperte Standardsoftware als bewegliche Sache gemäß § 90 BGB anzusehen, auf die je nach Überlassungsform Miet- oder Kaufrecht anwendbar ist.[53]

Die Daten sind rechtlich gesehen kein wesentlicher Bestandteil (vgl. § 93 BGB) des Speichermediums, auf dem sie abgespeichert sind.[54] Gemäß § 93 BGB können wesentliche Bestandteile einer Sache nicht Gegenstand besonderer Rechte sein; dabei handelt es sich um Bestandteile, die voneinander nicht getrennt werden können, ohne dass der eine oder der andere zerstört oder in seinem Wesen verändert wird.

[47] *Hoeren*, NJW 2005, S. 2113 (2114)
[48] *BGH*, NJW 2007, S. 2394, Rn. 19.
[49] *Herzog/Pruns*, in: Der digitale Nachlass, § 1 Rn. 27.
[50] *BGH*, NJW 2007, S. 2394, Rn. 19.
[51] *Herzog/Pruns*, in: Der digitale Nachlass, § 1 Rn. 39.
[52] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 32 f.
[53] *BGH*, NJW 2007, S. 2394
[54] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 32

5.3.1.4 Dateninhalte

Von den reinen Daten bzw. Dateien zu unterscheiden sind die darin enthaltenen, gespeicherten Informationen (etwa Texte, Bilder, Filme, Computerprogramme). Man kann insofern auch zwischen der Zeichenebene (bezüglich Daten und Dateien) und der Bedeutungsebene (bezüglich der Inhalte) differenzieren.[55] Diese Dateninhalte können Gegenstand eigener Rechte sein. Je nach Art des Dateninhalts können sich diese beispielsweise aus dem Persönlichkeitsrecht, Datenschutzrecht oder Immaterialgüterrecht ergeben.[56]

Digitale Inhalte, wie etwa Filme, Musik, Spiele oder andere Software, können auch unabhängig von einem körperlichen Datenträger geliefert werden. Gemäß der Legaldefinition des § 312f III BGB sind digitale Inhalte „nicht auf einem körperlichen Datenträger befindliche Daten, die in digitaler Form hergestellt und bereitgestellt werden".

Wie der BHG feststellte, folgt die Berechtigung an den gespeicherten Inhalten anderen Regeln als das Eigentum an den Speichermedien. Im vorliegenden Fall klagte Altkanzler Kohl gegen einen Journalisten, der seine Memoiren abfassen sollte, auf Herausgabe von Tonbändern mit dazu geführten Gesprächen. Der BGH erklärte, ihre Bedeutung und Einmaligkeit zeichneten nur die aufgenommenen Inhalte, aber nicht die Tonbänder als Speichermedien aus; die Inhalte besagten über die eigentumsrechtliche Zuordnung des Speichermediums nichts.[57]

Es ist daher zwischen dem Eigentumsrecht an der Sache (dem Datenträger) und eventuellen weiteren Rechten an Daten bzw. den digitalen Inhalten zu unterscheiden. Neben den relativen Rechtspositionen, also Rechten und Pflichten, die sich aufgrund zwischen den Parteien geschlossener Verträge ergeben, kann an den Daten bzw. Dateninhalten ein absoluter Schutz bestehen.[58] Infrage kommt u. a. das Urheberrecht, das den Urheber in seiner ideellen Beziehung zu seinem Werk schützt und ihn befugt, es angemessen zu verwerten (vgl. §§ 2, 11 UrhG).

5.3.2 Schutz durch das Urheberrecht

Zu den gemäß § 2 UrhG geschützten Werken der Literatur, Wissenschaft und Kunst gehören beispielsweise Sprach-, Musik-, Lichtbild- und Filmwerke. Computerprogramme fallen unter Sprachwerke (vgl. §§ 2 I Nr. 1, 69a UrhG).

5.3.2.1 Voraussetzungen des Schutzes

Das Urheberrecht schützt gemäß § 11 UrhG den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk (Urheberpersönlichkeitsrecht) und in der Nutzung des Werkes (Verwertungsrecht). Damit Urheberrechtsschutz entsteht, muss dementsprechend ein Werk vorliegen, also die

[55] *Herzog/Pruns*, in: Der digitale Nachlass, § 1 Rn. 27.
[56] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 32
[57] *BGH*, GRUR 2016, 109, Rn. 20
[58] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 35 , 55 ff.

wahrnehmbare Form[59] einer persönlichen geistigen Schöpfung (vgl. § 2 II UrhG). Um als urheberrechtlich schützenswertes Werk qualifiziert zu werden, muss die individuelle geistige Schöpfung ein gewisses Maß an Originalität besitzen (die erforderliche Schöpfungshöhe). Bei Werken, die gerade noch diese Bedingungen erfüllen, spricht man von der sogenannten „kleinen Münze“.

Urheberrechtlicher Schutz von Computer- bzw. Videospielen Der Quell- und Maschinencode des zugrunde liegenden Computerprogramms sind als literarisches Werk gemäß § 2 I Nr. 1, 69a UrhG schützenswert. Die audiovisuellen Bestandteile können Schutz als Filmwerk gemäß § 2 I Nr. 1 oder zumindest als Laufbilder gemäß § 95 UrhG genießen.[60]

Urheberrechtlicher Schutz von E-Books E-Books sind als literarisches Werk gemäß § 2 I Nr. 1 UrhG geschützt. Sie können aber auch neben dem reinen Text weitere selbstständig urheberrechtlich schutzfähige Elemente enthalten, etwa Grafiken, Videos oder Musikwerke.[61]

Urheberrechtlicher Schutz von Film- und Audiodateien Filme (§ 2 I Nr. 6) und Audiodateien (§ 2 I Nr. 2) erreichen in der Regel die erforderliche Schöpfungshöhe, um Urheberrechtsschutz zu erhalten.[62]

Filmaufnahmen, die die Voraussetzungen des § 2 UrhG nicht erfüllen und daher dem Urheberrechtsschutz nicht zugänglich sind, können dennoch Leistungsschutz als Laufbilder gemäß § 95 UrhG erhalten.[63] Darunter fallen beispielsweise dokumentarische Aufnahmen, bei denen es sich etwa nur um eine schematische Aufnahme und Wiedergabe chronologischer Abläufe handelt.[64]

5.3.2.2 Urheberrechtliche Verwertungsrechte

Die Verwertungsrechte der §§ 15 ff. UrhG schützen hauptsächlich die materiellen Interessen des Urhebers. § 15 UrhG gewährt dem Urheber ein allgemeines Verwertungsrecht. Er hat danach das ausschließliche, d. h. gegenüber jedermann wirkende Recht, sein Werk in körperlicher Form und in unkörperlicher Form zu verwerten. § 15 UrhG enthält zudem einen nicht abschließenden Katalog an besonderen Verwertungsrechten. Der Urheber kann anderen die Verwertung verbieten, sofern keine gesetzliche Erlaubnis entgegensteht (vgl. § 45 ff., 69d, 69e UrhG). Er kann anderen den Verwertungsrechten entsprechende Nutzungsrechte (vgl. §31 ff UrhG) einräumen. Nutzungsrechte können für einzelne oder alle Nutzungsarten, als einfaches oder ausschließliches Recht sowie räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden (vgl. 31 UrhG).

[59] Reine Ideen werden nicht geschützt, nur deren wahrnehmbare Ausprägung.
[60] *Schapiro*, in: *Bräutigam/Rücker*, E-Commerce, 6. Teil, F., Rn. 3 ff.
[61] *Schapiro* in: *Bräutigam/Rücker*, E-Commerce, 6. Teil, B., Rn. 4 f.
[62] *Schapiro*, in: *Bräutigam/Rücker*, E-Commerce, 6. Teil, C., Rn. 3.
[63] Neben dem Urheberrecht kennt Teil 2 des UrhG die verwandten Schutzrechte, auch Leistungsschutzrechte genannt. Diese ausschließlichen Rechte dienen insbesondere dem Investitionsschutz.
[64] *Manegold/Czernik*, in: Wandtke/Bullinger, UrhG, § 95 Rn. 4, 6.

5.3.2.3 Verwertung in körperlicher Form

Zur Verwertung des Werkes in körperlicher Form (vgl. § 15 I UrhG) zählen u. a. das Vervielfältigungsrecht (vgl. § 16 UrhG) und das Verbreitungsrecht (vgl. § 17 UrhG).

Vervielfältigungsrecht Beim Vervielfältigungsrecht handelt es sich um das Recht, Vervielfältigungsstücke des Werkes herzustellen, gleichviel ob vorübergehend, dauerhaft oder in welchem Verfahren (vgl. § 16 I UrhG). Bei digitalisierten Werken ist z. B. jede Speicherung, unabhängig von Speichermedium und Format, eine Vervielfältigung, auch wenn dies per Download von bzw. Upload auf Server geschieht. Auch die Digitalisierung von Werken, etwa durch Scannen, ist eine Vervielfältigung. Ebenso stellt die Zwischenspeicherung im Arbeitsspeicher des Computers eine Vervielfältigung dar. Gemäß der Schranke des § 44a UrhG sind vorübergehende Vervielfältigungen, die flüchtig oder begleitend sind und wesentlich für den technischen Prozess sind, zulässig, soweit sie nur den Zweck haben, den rechtmäßigen Gebrauch zu ermöglichen und keine eigene wirtschaftliche Bedeutung haben.[65]

Verbreitungsrecht Das Verbreitungsrecht ist das Recht, das Original oder Vervielfältigungsstücke des Werkes der Öffentlichkeit anzubieten oder in Verkehr zu bringen. Das Verbreitungsrecht ist nur bei Eigentumsübertragung des Originals oder Vervielfältigungsstücks betroffen, nicht bei Besitzübertragung (z. B. Miete).[66]

5.3.2.4 Verwertung in unkörperlicher Form

§ 15 II UrhG enthält einen Beispielkatalog für Verwertung des Werkes in unkörperlicher Form durch öffentliche Wiedergabe. Ein Unterfall der Verwertung in unkörperlicher Form ist u. a. das Recht der öffentlichen Zugänglichmachung. Dieses Recht ist relevant für die Werknutzung in elektronischen Netzen, insbesondere im Internet.[67]

Gemäß § 19a UrhG sowie der Spezialnorm für Software, § 69c Nr. 4 UrhG, ist dieses Recht betroffen, wenn das Werk drahtgebunden oder drahtlos der Öffentlichkeit derart zugänglich gemacht wird, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist. Laut § 15 III UrhG ist die Wiedergabe öffentlich, wenn sie für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist.[68] Dies bedeutet nicht, dass es auch tatsächlich von allen die Öffentlichkeit umfassenden Personen zur Kenntnis genommen wird. Werden beispielsweise fremde Werke ohne Erlaubnis auf einer Homepage wiedergegeben oder zum Download angeboten, wird das Recht auf öffentliche Zugänglichmachung verletzt. § 19a UrhG ist u. a. auch einschlägig beim Verfügbarmachen von

[65] Für vorstehenden Absatz, *Heerma*, in: Wandtke/Bullinger, UrhG, § 16, Rn. 16 ff.
[66] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 14 ff.
[67] *Bullinger*, in: Wandtke/Bullinger, UrhG, § 19a, Rn. 6.
[68] Zur Öffentlichkeit gehört gemäß § 15 III jeder, der nicht mit demjenigen, der das Werk verwertet, oder mit den anderen Personen, denen das Werk in unkörperlicher Form wahrnehmbar oder zugänglich gemacht wird, durch persönliche Beziehungen verbunden ist.

Podcast-Audiodateien auf einem Server oder bei On-Demand-Diensten wie etwa Video-on-Demand und Audio-on-Demand.[69]

5.3.3 Der urheberrechtliche Erschöpfungsgrundsatz

Während der Download eines Werkes (wie die dauerhafte Speicherung eines E-Books auf den E-Book-Reader) eine Vervielfältigung gemäß § 16 I UrhG darstellt, ist bei Verkauf urheberrechtlich geschützter Werke in körperlicher Form, also z. B. eines gedruckten Buches oder einer CD, das Verbreitungsrecht gemäß § 17 I UrhG betroffen.

Das Urheberrecht und damit auch die Verwertungsrechte sind teilweise zum Ausgleich der Interessen des Urhebers und privater oder allgemeiner Interessen beschränkt.[70]

Der Erschöpfungsgrundsatz des § 17 II UrhG (bzw. des § 69c Nr. 3 S. 2 als Spezialnorm für Computerprogramme) beschränkt die Reichweite des Verbreitungsrechts.[71] Wurde das Original eines Werkes oder sein Vervielfältigungsstück mit Zustimmung des Urhebers bzw. Rechteinhabers im Gebiet der EU oder des EWR im Wege der Veräußerung in Verkehr gebracht, kann der Rechteinhaber dessen Weiterverkauf nicht mehr verbieten. Denn das Verbreitungsrecht des Urhebers bzw. Rechteinhabers an diesem bestimmten Werkexemplar ist erschöpft und die Weiterverbreitung ist – mit Ausnahme der Vermietung – somit ohne dessen Zustimmung zulässig (vgl. § 17 II S. 2 , § 69c Nr. 3 S. 2 UrhG). Wurde also z. B. ein gedrucktes Buch, ein Film auf DVD, Musik oder Standardsoftware auf einer CD oder einem anderen Datenträger mit Zustimmung des Rechteinhabers in Verkehr gebracht, darf der jeweilige Käufer dieses Exemplar entsprechend weiterverbreiten.

Der Erschöpfungsgrundsatz begrenzt die Behinderungen des Warenverkehrs aufgrund des Verbreitungsrechts und dient dem Interessenausgleich zwischen dem Urheberrecht und dem Eigentumsrecht an dem Werkexemplar. Der Erblasser kann insoweit gemäß seinem Eigentumsrecht über dieses Exemplar frei verfügen.[72]

Den wirtschaftlichen Interessen des Urhebers wurde dadurch genügt, dass er bei der ersten Veräußerung die Möglichkeit hatte, eine Vergütung zu verlangen.[73] Der Weiterverkauf eines einzelnen Werkexemplars hat keinen Einfluss auf das Urheberrecht selbst.[74]

Die übrigen Verwertungsrechte werden durch die Erschöpfung grundsätzlich nicht berührt.[75]

[69] *Bullinger*, in: Wandtke/Bullinger, UrhG, § 19a, Rn. 22–26.
[70] Solche Schrankenbestimmungen, wie etwa das Recht auf „Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch“, beinhalten insbes. die §§ 44a ff. UrhG.
[71] Für Datenbanken gilt § 87b II UrhG entsprechend.
[72] *Herzog/Pruns* in: Der digitale Nachlass, § 3 Rn. 12.
[73] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 27.
[74] *Herzog/Pruns*, in: Der digitale Nachlass, § 3 Rn. 12.
[75] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 36.

5.3.3.1 Tatbestandsvoraussetzungen der Erschöpfung

Veräußerung

Veräußerung i. S. d. §§ 17 II S. 2, 69c Nr. 3 S. 2 UrhG bezieht sich nicht nur auf kaufrechtliche Überlassungsverträge (vgl. § 433 ff BGB), sondern umfasst in der Regel jede rechtsgeschäftliche Übertragung des Eigentums durch den Urheber bzw. Rechteinhaber (z. B. auch Tausch und Schenkung). Miete und Leihe führen nicht zur Erschöpfung.[76]

Zustimmung

Für die Zustimmung gelten die §§ 182 ff. BGB. Der Rechteinhaber kann dem Inverkehrbringen durch Veräußerung durch Einwilligung im Voraus zustimmen und es im Nachhinein genehmigen.[77]

Räumliche Beschränkung

Das Werkstück muss auf dem Gebiet der EU oder eines Vertragsstaates des EWR in Verkehr gebracht worden sein. Bei Erstveräußerung außerhalb der EU und des EWR tritt keine Erschöpfung ein.[78]

Original oder Vervielfältigungsstück

Nach dem Wortlaut der §§ 17 und 69c UrhG betrifft die Erschöpfung immer konkrete Werk- oder Vervielfältigungsstücke, die veräußert wurden. Nur für das jeweilige konkrete Exemplar ist das Verbreitungsrecht erschöpft, nicht für alle anderen Vervielfältigungsstücke.[79] Die Erschöpfung erstreckt sich auch nicht auf rechtmäßig hergestellte Vervielfältigungsstücke wie etwa Sicherungskopien von Computerprogrammen.[80]

Kontrovers diskutiert wird die Frage, ob der Erschöpfungsgrundsatz auch im Online-Bereich anzuwenden ist, wenn die Erstveräußerung in unkörperlicher Form per Datenübertragung stattfindet.

5.3.3.2 Diskussion der Erschöpfung von unkörperlich in Verkehr gebrachten Werken

Computerprogramme

Hinsichtlich Software, die per Download erworben wurde, wurde auf höchstrichterlicher Ebene der Erschöpfungsgrundsatz bejaht. Aufgrund eines Vorabentscheidungsersuchens des BGH stellte der EUGH in der UsedSoft-Entscheidung fest, das Verbreitungsrecht an einer Kopie eines Computerprogramms sei auch dann erschöpft, wenn der Inhaber des Urheberrechts dem Herunterladen der Kopie

[76] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 28 f; *Grützmacher*, in: Wandtke/Bullinger, UrhG, § 69c, Rn. 33.
[77] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 34.
[78] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 35. Die Beschränkung gilt u. a. auch gemäß § 69c Nr. 3 S. 2 UrhG.
[79] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 29.
[80] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 29, mit Verweis auf EuGH, MMR 2017, S. 19.

aus dem Internet zugestimmt habe und gleichzeitig dem Ersterwerber ein zeitlich unbegrenztes Nutzungsrecht für diese Kopie gegen Zahlung eines Entgelts vertraglich eingeräumt habe.[81] Durch diese Geschäfte werde das Eigentum an der Kopie übertragen.[82] Der BGH verfasste in seinem im Anschluss ergangenen Urteil[83] („UsedSoft III“) u. a. folgenden Leitsatz: „Ist ein körperliches oder ein unkörperliches Vervielfältigungsstück eines Computerprogramms mit Zustimmung des Rechtsinhabers im Wege der Veräußerung in Verkehr gebracht worden, ist die Weiterverbreitung aufgrund der eingetretenen Erschöpfung des urheberrechtlichen Verbreitungsrechts ungeachtet einer inhaltlichen Beschränkung des eingeräumten Nutzungsrechts frei.“ Der Ersterwerber muss zum Zeitpunkt des Weiterverkaufs seine eigene Kopie unbrauchbar machen, um nicht das ausschließliche Recht des Urhebers auf Vervielfältigung des Computerprogramms zu verletzen.[84] Wurde die heruntergeladene Software auf einem Server installiert und hat der Ersterwerber eine Lizenz zur Nutzung durch mehrere Nutzer erworben, kann sich der Nacherwerber nur auf die Erschöpfung berufen, wenn der Ersterwerber seine Kopie unbrauchbar gemacht hat.[85] Bei einer Lizenz zur Nutzung mehrerer eigenständiger Kopien kann der Nacherwerber von Kopien sich nur dann auf die Erschöpfung des Verbreitungsrechts berufen, wenn der Ersterwerber eine entsprechende Anzahl unbrauchbar gemacht hat.[86] Darüber hinaus muss der Nacherwerber, der sich etwa im Bestreitensfall auf den Erschöpfungsgrundsatz beruft, sämtliche tatsächlichen Voraussetzungen des jeweiligen konkreten Einzelfalls kumulativ darlegen und beweisen können, u. a. die Zustimmung des Rechteinhabers zum Download des Computerprogramms durch den Ersterwerber und Erteilung eines zeitlich unbegrenzten Nutzungsrechts, gegebenenfalls, dass der Download von Updates durch den Nacherwerber von einem zwischen Rechteinhaber und Ersterwerber abgeschlossenen Wartungsvertrag gedeckt ist, und dass der Nacherwerber die Programmkopie nur in dem Ersterwerber vertraglich gestatteten, bestimmungsgemäßen Umfang nutzt.[87]

In einem weiteren Urteil stellte der BGH fest, dass die Erschöpfung des Verbreitungsrechts an einer Kopie eines Computerprogramms gemäß § 69c Nr. 3 S. 2 UrhG sich sowohl auf das Recht erstreckt, die Programmkopie auf einem Datenträger weiterzugeben, als auch auf die Veräußerung durch Bekanntgabe eines zum Herunterladen des Programms erforderlichen Produktschlüssels. Darauf, ob der Ersterwerber seine Kopie vom Verkäufer durch Übergabe eines Datenträgers oder durch Bekanntgabe des Produktschlüssels erhalten habe, käme es nicht an.[88]

Bezüglich Computerprogrammen kann der Rechteinhaber die Veräußerung daher i. d. R. nicht in seinen AGB verbieten. Denn Verwendungsbeschränkungen in AGB, die die Erschöpfungswirkung aushebeln, sind regelmäßig unwirksam.[89]

Laut einem Beschluss des OLG Hamburg ist etwa die Klausel, „Außerdem sind Sie berechtigt, die

[81] *EUGH*, NJW 2012, S. 2565.
[82] *EUGH*, NJW 2012, S. 2565, Rn. 44 ff.
[83] *BGH*, GRUR 2015, S. 772.
[84] *EUGH*, NJW 2012, S. 2565, Rn. 70.
[85] *BGH*, GRUR 2015, S. 772.
[86] *BGH*, GRUR 2015, S. 772.
[87] *OLG München*, MMR 2015, S. 397.
[88] *BGH*, GRUR 2015, S. 1108.
[89] *OLG Hamburg*, MMR 2014, S. 115 (116).

Software (zusammen mit der Lizenz) auf einen Computer zu übertragen, der jemand anderem gehört, wenn a) Sie der erste Lizenznehmer der Software sind und b) der neue Nutzer den Bestimmungen dieses Vertrages zustimmt“, gegenüber Verbrauchern unwirksam. Sie verstößt laut dem OLG gegen § 307 I S. 1, II Nr. 1 BGB, denn sie benachteiligt die Vertragspartner entgegen Treu und Glauben unangemessen, indem sie von der gesetzlichen Regelung des § 69c Nr. 3 S. 2 UrhG abweicht und mit deren wesentlichen Grundgedanken nicht zu vereinbaren ist. Nach o. g. Klausel dürfte die Software nur vom ersten Lizenznehmer weiterveräußert werden. Zudem müsste der Nacherwerber den Bestimmungen des Lizenzvertrags zustimmen. Damit werde die Weiterveräußerung der Software über die erste Stufe hinaus untersagt und im Übrigen unter eine Bedingung gestellt (Zustimmung zum Lizenzvertrag), die in der gesetzlichen Regelung nicht vorgesehen ist.[90]

Digitale Kopien anderer Werkkategorien

Die Frage, ob der Erschöpfungsgrundsatz auch bezüglich sonstiger Werkexemplare gilt, wenn die Vervielfältigungsstücke erst auf Speichermedien der Empfänger gespeichert werden, ist umstritten (etwa bei durch Online-Download erworbenen Büchern, Filmen, Spielen oder Musik).

Keine Veräußerung und damit keine Erschöpfung liegt jedenfalls vor, wenn der Nutzer zwar online Zugang zum Werk erhält, dieses ihm aber nicht zum Download auf einen eigenen Datenträger, sondern allenfalls als flüchtige Kopie zur Verfügung gestellt wird, insbesondere beim Streaming.[91] Dabei findet keine Übertragung des Eigentums der Daten an den Nutzer statt, sie bleiben unter faktischer Kontrolle eines anderen.[92]

Auf europarechtlicher Ebene finden für Computerprogramme und sonstige Werkkategorien zwei verschiedene Richtlinien Anwendung. So bezog sich die UsedSoft-Entscheidung des EuGH auf die sogenannte Software-Richtlinie.[93] Diese ist im Verhältnis zur sogenannten InfoSoc-Richtlinie,[94] die für andere Werkarten einschlägig ist, als lex specialis zu betrachten. Der EuGH bezog sich insbesondere auf Art. 4 II der Software-Richtlinie und den deutlichen Willen des Unionsgesetzgebers, im Hinblick auf den vorgesehenen Schutz körperliche und nichtkörperliche Programmkopien einander gleichzustellen.[95] Die Frage der Erschöpfung für andere Werkkategorien wurde offengelassen.[96]

Die herrschende Meinung in Rechtsprechung und Literatur spricht sich gegen eine Übertragung des Erschöpfungsgrundsatzes auf Downloads sonstiger Werkkategorien aus.[97] U. a. wird argumentiert, die UsedSoft-Entscheidung des EuGH sei nicht auf andere Werkarten übertragbar.

[90] *OLG Hamburg*, MMR 2014, S. 115 (116).
[91] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 33; *Hilty*, GRUR 2018, S. 865 (866).
[92] *Hilty*, GRUR 2018, S. 865 (866).
[93] Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen.
[94] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.
[95] *EuGH*, MMR 2012, S. 586 (588), Rn. 57 ff.
[96] *EuGH*, MMR 2012, S. 586 (588), Rn. 60.
[97] Zum Meinungsstand in Rechtsprechung und Literatur, Heerma, in: Wandtke/Bullinger, UrhG, § 17, Rn. 30.

So sind etwa nach der Rechtsprechung des OLG Hamburg[98] und des OLG Hamm[99] AGB-Klauseln, die die Weiterveräußerung digitaler Güter (wie E-Books und Hörbücher bzw. Audiodateien) verbieten, keine unangemessene Benachteiligung gemäß § 307 BGB und daher wirksam. Bezüglich der Downloads trete per se keine Erschöpfung ein, weil nicht § 17, sondern § 19a UrhG einschlägig sei und diese Bestimmung bewusst und gewollt keine Erschöpfung des Verbreitungsrechts kenne. Eine europarechtskonforme Auslegung des § 17 II UrhG gemäß Art. 4 II der InfoSoc-Richtlinie ergebe, dass § 17 II UrhG lediglich körperliche Werkstücke umfasse.

Dagegen besagt eine andere Ansicht, die teilweise in der Literatur vertreten wird, dass zumindest die körperliche Weitergabe des heruntergeladenen Werkstücks vom Erschöpfungsgrundsatz erfasst sei, also die online übermittelte Kopie, die sich auf dem Speichermedium der Hardware befindet, welche der Ersterwerber veräußert. Gerade bei E-Books sei eine Einschränkung der Rechte des Käufers im Vergleich zu gedruckten Büchern wirtschaftlich kaum zu rechtfertigen. Die Herstellungs- und Vertriebskosten seien bei E-Books im Vergleich zu gedruckten Büchern viel niedriger, sie würden aber wegen der Buchpreisbindung zu denselben Preisen vertrieben.[100]

Der Generalanwalt beim EuGH kommt in seinem Schlussantrag[101] vom 10.09.2019 zu dem Ergebnis, dass der Erschöpfungsgrundsatz auf Downloads nicht anwendbar ist. Im vorliegenden Fall, einem Vorabentscheidungsersuchen der Rechtbank Den Haag gegen eine Plattform für „gebrauchte“ E-Books („Tom Kabinet“), empfiehlt der Generalanwalt dem EuGH folgende Antwort auf die Vorlagefrage: „Art. 3 I und Art. 4 der InfoSoc-Richtlinie sind dahin auszulegen, dass die Überlassung von E-Books zur dauerhaften Nutzung durch Herunterladen aus dem Internet nicht dem Verbreitungsrecht im Sinne von Art. 4 der Richtlinie unterliegt, sondern dem Recht der öffentlichen Wiedergabe im Sinne von Art. 3 I der Richtlinie.“[102]

Es gebe zwar sowohl teleologische als auch rechtliche Argumente für die Anwendung der Erschöpfung des Verbreitungsrechts auf Werke, die durch Herunterladen dauerhaft überlassen werden. Insbesondere der dauerhafte Besitz des Nutzers an der so überlassenen Kopie sei ein Beleg für die Vergleichbarkeit mit der Verbreitung körperlicher Kopien. Jedoch müssten die Gegenargumente beim derzeitigen Stand des Europarechts den Vorrang haben.[103] So sei Erwägungsgrund 29 der InfoSoc-Richtlinie insoweit unmissverständlich, als nach dem Willen des europäischen Gesetzgebers auf alle Formen der Online-Verwertung von Werken das Recht der öffentlichen Wiedergabe (in der Form der öffentlichen Zugänglichmachung) Anwendung finde. Dies gelte sowohl auf Verwertungsformen, die an keine Kopie gebunden seien, als auch auf diejenigen, die auf der Erstellung einer Kopie beruhten.[104]

Der Generalanwalt hält das UsedSoft-Urteil auf E-Books nicht für anwendbar. Ein E-Book sei kein

[98] *OLG Hamburg*, ZUM 2015, S. 503.
[99] *OLG Hamm*, NJW 2014, S. 3659.
[100] *Heerma*, in: Wandtke/Bullinger, UrhG, § 17, Rn. 32.
[101] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448.
[102] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448.
[103] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448.
[104] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 39.

Computerprogramm, also keine Reihe von Befehlen an den Computer, bestimmte Operationen auszuführen, sondern es sei eine digitale Datei mit Daten, die der Computer zu verarbeiten habe.[105]

Die Digitalisierung und die technische Entwicklung führten zu einer Erschütterung des Gleichgewichts zwischen den Interessen der Rechtsinhaber und der Nutzer. Exakte digitale Kopien seien zu geringen Kosten herstellbar und mühelos über das Internet übertragbar. Dies stelle die Möglichkeit der Urheberrechtsinhaber infrage, eine angemessene Vergütung zu erhalten und begünstige die Herstellung von Raubkopien. Andererseits könnten die Rechteinhaber durch moderne Technologien die Erwerber weitgehend kontrollieren und Geschäftsmodelle entwickeln, durch die die uneingeschränkte Nutzung der Kopie in ein beschränktes und bedingtes Nutzungsrecht umgewandelt werde – ohne dies offenzulegen.[106]

Zwar bestünden erhebliche Gründe für die Anerkennung der Erschöpfung des Verbreitungsrechts für digitale Downloads, jedoch stünden andere Gründe mit zumindest gleichem Gewicht dagegen. Dieses Interessengleichgewicht führe daher dazu, dass die Abwägung nicht anders ausfalle, als dies vom Wortlaut der geltenden Bestimmungen vorgegeben sei.[107]

Nach Ansicht des Generalanwalts würde der EuGH mit der Anerkennung des Erschöpfungsgrundsatzes im Bereich des Internets ein Problem lösen, das nicht wirklich gelöst zu werden brauche und weitgehend der Vergangenheit angehöre.[108]

Das mit einem dauernden Nutzungsrecht verbundene Herunterladen als Form der Überlassung von Inhalten sei im Begriff, der Vergangenheit anzugehören. Neue Zugangsmöglichkeiten wie das Streaming oder Online-Abonnements würden von den Urheberrechtsinhabern, den Vertreibern und den Nutzern positiv aufgenommen.[109] Bezüglich E-Books sei das Streaming schwierig zu konzipieren, doch existierten bereits Lösungen, bei denen ein Nutzer durch Zahlung einer periodischen Abonnementgebühr Zugang zu einer ganzen E-Book-Bibliothek erhalte. Dafür sei zwar der Download des E-Books erforderlich, doch es müsse nicht für jedes heruntergeladene Objekt eine Zahlung geleistet werden, und daher könne kaum von einem „Verkauf“ gesprochen werden.[110]

5.3.3.3 Verschiedene Generationen digitaler Werknutzung

Wie o. g. Schlussantrag des Generalanwalts zu entnehmen ist, hat sich die Art der Online-Nutzung mit der Zeit verändert, was sich auch auf die vertragstypologische Einordnung auswirkt:

Unterteilt man die Technologien zur Nutzung digitaler Werke in drei – derzeit koexistierende – Generationen bzw. Phasen, wurden in der ersten Phase die Werkexemplare anstatt auf analogen Datenträgern auf digitalen Datenträgern vertrieben, z. B. wurden Vinylplatten oder Magnetbänder durch

[105] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 67.
[106] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 4 ff.
[107] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 97.
[108] *EuGH*, Schlussantrag Generalanwalt Szpunar v. 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 96.
[109] EuGH, Schlussantrag Generalanwalt Szpunar v. 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 95.
[110] *EuGH*, Schlussantrag Generalanwalt Szpunar vom 10.9.2019, C-263/18, BeckRS 2019, S. 20448, Rn. 95.

CDs bzw. durch DVDs ersetzt. Bei dieser Vertriebsform steht nach wie vor das Kaufrecht im Vordergrund.[111]

In der zweiten Phase bereiteten die Anbieter den Nutzern die Möglichkeit, die Werkkopien über das Internet herunterzuladen und auf eigenen Datenträgern abzuspeichern. Die Vervielfältigungsstücke wurden also vom jeweiligen Nutzer selbst hergestellt. Auch bei dieser Vertriebsform ist nach herrschender Ansicht (zumindest analog) von der Anwendbarkeit des Kaufrechts auszugehen.[112]

In der dritten Phase, zu der insbesondere das Streaming zählt, werden höchstens noch flüchtige Vervielfältigungen (etwa auf dem Bildschirm oder im Arbeitsspeicher) hergestellt. Beim Nutzer entsteht keine dauerhafte Programmkopie mehr, auf die er wiederholt zurückgreifen kann. Er kann nur auf Daten zugreifen und diese vorübergehend nutzen.[113]

Daneben gibt es Geschäftsmodelle, die eine Kombination der Merkmale der o. g. Phasen beinhalten. Dabei können Daten zwar zeitlich befristet heruntergeladen werden, diese werden aber nach einer bestimmten Zeitspanne oder bei Abonnementsende automatisch gelöscht oder unbrauchbar gemacht. Die Nutzer können in der Regel keine Vervielfältigungen herstellen und die Inhalte nicht dauerhaft und unabhängig nutzen.[114] Wie bei der dritten Phase scheidet hier die typologische Einordnung als Kaufvertrag aus, da schon keine dauerhafte Überlassung (vgl. §§ 433, 453 BGB) der Daten erfolgt.

Tritt bei der unkörperlichen Erstverbreitung keine Erschöpfung ein, weichen derartige Klauseln auch insofern nicht vom wesentlichen Grundgedanken der gesetzlichen Regelung des § 17 II UrhG ab (vgl. 307 II Nr. 1 BGB). Das AGB-Recht steht einer solchen Klausel grundsätzlich nicht entgegen.[115]

In der Rechtsprechung wurden entsprechende Klauseln auch für zulässig erklärt. So entschied das OLG Hamm, dass in den Allgemeinen Geschäftsbedingungen eines Anbieters zu Hörbüchern, die von Kunden heruntergeladen und auf eigenen Datenträgern gespeichert werden, folgende Formulierungen nicht zu beanstanden sind: a) „Im Rahmen dieses Angebots erwirbt der Kunde das einfache, nicht übertragbare Recht, die angebotenen Titel zum ausschließlich persönlichen Gebrauch gemäß Urheberrechtsgesetz in der jeweils angebotenen Art und Weise zu nutzen.“ b) die Formulierung, die dem Kunden untersagt, die Datei(en) „für Dritte zu kopieren“ oder „weiterzuverkaufen“.[116]

Bezüglich entgeltlichen Musikdownloads beinhaltet laut einem Urteil des LG Berlin eine AGB-Klausel, die den Weitervertrieb, die Weitergabe, Übergabe oder Unterlizenzierung vorbehaltlich abweichender gesetzlicher Regeln verbietet, keine unangemessene Benachteiligung, da keine Erschöpfung eintritt.[117] Die Berufungsinstanz hielt die konkrete Klausel zwar bereits wegen Intransparenz gemäß § 307 I, II BGB für unwirksam,[118] merkte aber an, dass die Klausel jeder sachlichen Inhaltskontrolle

[111] Für vorstehenden Absatz: *Hilty*, GRUR 2018, S. 865 (866), mit weiteren Verweisen zur Annahme des Kaufrechts.
[112] *Hilty*, GRUR 2018, S. 865 (866), mit weiteren Verweisen zur Annahme des Kaufrechts.
[113] *Hilty*, GRUR 2018, S. 865 (866).
[114] *Hilty*, GRUR 2018, S. 865 (866).
[115] *Hilty*, GRUR 2018, S. 865 (877).
[116] *OLG Hamm*, NJW 2014, S. 3659.
[117] *LG Berlin*, GRUR-RR 2009, S. 329.
[118] *LG Berlin*, GRUR-RR 2009, S. 329.

standhielte, weil sie ihrem Wortlaut nach den Vertragspartner nur im von Gesetzes wegen gerade noch zulässigen Ausmaß benachteilige.[119]

Der BGH hat bezüglich eines Computerspiels („Half-Life 2“), das zwar auf DVD verkauft wurde, dessen vollumfängliche Nutzung aber nur möglich war, nachdem der Erwerber der DVD online auf der Webseite der Beklagten ein Nutzerkonto eingerichtet hat, folgenden Leitsatz formuliert: „Der urheberrechtliche Grundsatz der Erschöpfung des Verbreitungsrechts wird nicht berührt, wenn der Berechtigte das von ihm geschaffene, auf DVD vertriebene Computerspiel so programmiert, dass es erst nach der online erfolgten Zuweisung einer individuellen Kennung genutzt werden kann, und wenn er sich vertraglich ausbedingt, dass diese Kennung nicht an Dritte weitergegeben werden darf. Dies gilt auch dann, wenn die DVD mit dem Computerspiel wegen der ohne Kennung eingeschränkten Spielmöglichkeiten vom Ersterwerber praktisch nicht mehr weiterveräußert werden kann.“[120]

Die Nutzung digitaler Inhalte wird inzwischen von den meisten Anbietern dadurch beschränkt, dass zu ihrem Erwerb bei dem Anbieter ein Nutzerkonto eröffnet werden muss, das in der Regel laut ihren Nutzungsbedingungen nicht übertragen werden darf. Spätestens in der dritten Phase geht es primär um die Frage des Zugangs zu Daten bzw., ob die Nutzungsberechtigung, die der Rechteinhaber dem Vertragspartner eingeräumt hat, auch gegen den Willen des Rechteinhabers auf einen Dritten übertragbar ist.[121]

Bezüglich des Übergangs des Zugangs zu Online-Nutzerkonten bzw. die Vererbbarkeit eines schuldrechtlichen Nutzungsverhältnisses gemäß § 1922 BGB ist das Facebook-Urteil des BGH richtungsweisend.

Aus der Darstellung folgt, dass an einzelnen Inhalten urheberrechtliche Einschränkungen bestehen können – selbst wenn das schuldrechtliche Nutzungsverhältnis grundsätzlich vererblich ist, können dennoch auch Urheberrechte Dritter gelten, etwa an Werkkopien, die der Nutzer in seinen Cloudspeicher hochgeladen hat. Der Erschöpfungsgrundsatz findet bezüglich Online-Downloads nur auf Computerprogramme Anwendung, nicht auf Werke wie beispielsweise E-Books, Filme oder Musik. Unter die Spezialnorm des § 69c Nr. 3 S. 2 UrhG fallen auch keine Software beinhaltenden multimedialen Werke. Zum Beispiel für Computerspiele ist § 17 II UrhG einschlägig. Wie obenstehende Beispiele aus der Rechtsprechung zeigen, sind Klauseln in Nutzungsbedingungen, die die Übertragung auf Dritte ausschließen, grundsätzlich wirksam. Auch sind viele Nutzungsverhältnisse mietvertraglich ausgestaltet. Daraus ist zu schließen, dass der Rechteinhaber die Nutzung urheberrechtlich geschützter Inhalte in den AGB auf die Lebenszeit des Nutzers begrenzen kann (vgl. § 31 UrhG).

[119] Konkret ging es um die Klausel „Der Weitervertrieb, die Weitergabe, Übertragung oder die Unterlizenzierung ist vorbehaltlich abweichender zwingender gesetzlicher Regeln nicht gestattet.“ Dadurch sollten dem Erwerber alle durch urheberrechtliche Schranken (§§ 44a ff. UrhG) eingeräumte Rechte entzogen werden, soweit gesetzlich zulässig, d. h. soweit der Erwerber dadurch nicht unangemessen benachteiligt wird. Das KG stellte fest, durch Hinzufügung des Wortes „zwingende“ werde die Rechtslage für den Erwerber undurchschaubar, da er nicht wissen könne, welche Beschränkung gesetzlicher Erlaubnisse die Beklagte als unangemessene Benachteiligung ansehe und vom generellen Verbot ausnehmen wolle.

[120] *BGH*, GRUR 2010, S. 822; ebenso für die Wirksamkeit einer Verbotsklausel: GRUR-RS 2016, S. 03668.

[121] *Hilty*, GRUR 2018, S. 865 (865 f.).

5.3.4 Rechtsnachfolge

Aus erbrechtlicher Sicht sind nach Auffassung des BGH digitale Inhalte nicht anders zu behandeln als analoge Inhalte. Auf das Speicher- bzw. Trägermedium kommt es nicht an. Eine Differenzierung zwischen höchstpersönlichen und sonstigen Inhalten würde zu kaum zu bewältigenden praktischen Problemen führen. Da E-Mail- und andere Benutzerkonten (z. B. für Cloudspeicherplatz) regelmäßig nicht ausschließlich höchstpersönlichen oder vermögensrechtlichen Zwecken dienen, wäre eine Durchsicht und Zuordnung sämtlicher digitaler Inhalte erforderlich, wobei fraglich wäre, wer diese vornehmen sollte bzw. die rechtliche Kompetenz dafür besäße.[122] Zudem kann ein und dieselbe Information sowohl ideelle als auch vermögenswerte Anteile beinhalten.[123] Auch eine Differenzierung danach, ob der digitale Inhalt auf einem lokalen Speichermedium gespeichert ist oder sich auf Servern eines Dienstanbieters befindet, lehnt der BGH mit der Begründung ab, dies wäre inkohärent und durch das Gesetz nicht veranlasst. Unterschiedlich ist demnach lediglich die Art und Weise der Vererbbarkeit:

- Bei Schriftstücken oder Speichermedien, die sich im Eigentum bzw. Besitz des Erblassers befinden, gehen diese auf die Erben über.
- Befinden sich die Inhalte auf Servern von Dienstanbietern, treten die Erben in das Vertragsverhältnis ein.[124]

Gemäß § 1922 BGB gehen grundsätzlich sämtliche Rechtspositionen, die der Erblasser innehatte, auf die Erben über.[125] Neben vermögensrechtlichen Inhalten gehen dabei auch Rechtspositionen mit höchstpersönlichen Inhalten unabhängig von einem Vermögenswert über, wie sich aus § 2047 II und § 2373 S. 2 BGB ergibt.[126] Wie bei einem klassischen Bankkonto gehen auch Nutzungsverhältnis und Guthaben eines Online-Kontos und Online-Zahldienstes auf die Erben über. Dabei ist es unerheblich, ob dies klassische oder neue Währungen wie Bitcoins betrifft.[127]

5.3.4.1 Rechte an den Inhalten

Generell können auf die Erben nur die vererblichen Rechte an den Informationen übergehen, die der Erblasser selbst an ihnen hatte. So darf beispielsweise der Käufer einer Film-DVD oder einer Musik-CD diese zwar verkaufen, ohne dabei eine Urheberrechtsverletzung zu begehen, er darf sie aber u. a. nicht vermieten (vgl. 17 III UrhG) oder öffentlich vorführen (vgl. § 19 IV UrhG), was für den Erben ebenso gilt. Auch die öffentliche Zugänglichmachung von Werkkopien auf Internet-Plattformen verstößt gegen § 19a UrhG, wenn dem Nutzer dieses nicht eingeräumt wurde. Cloud-Speicherungen,

[122] *BGH*, NJW 2018, S. 3178 (3183) Rn. 51.
[123] *Gomille*, ZUM 2018, S. 660 (664).
[124] *BGH*, NJW 2018, S. 3178 (3183) Rn. 50.
[125] *Herzog/Pruns*, in: Der digitale Nachlass, § 2 Rn. 31, 34.
[126] *BGH*, NJW 2018, S. 3178 (3183) Rn. 49.
[127] Für vorstehenden Absatz: *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn. 24.

die ein Nutzer zu rein privaten Zwecken vornimmt, können unter die Privatkopie-Schranke fallen, sofern die Vorgaben des § 53 UrhG beachtet werden.[128]

5.3.4.2 Cloud als allg. Speicherplatz

Hochladen von Werkkopien durch den Nutzer

Bezüglich (über das Internet zugänglichen) Cloud-Speicherplatz ist zunächst der Nutzer gegenüber dem Betreiber alleiniger Berechtigter an den gespeicherten Inhalten, unabhängig davon, ob daran evtl. Rechte Dritter bestehen. Sind Dritte Rechteinhaber, können sie gegebenenfalls gegenüber dem Nutzer Rechte geltend machen, etwa einen Anspruch auf Löschung oder Herausgabe (siehe dazu Kapitel 4.2.2 auf Seite 106).[129]

Entsprechend dem Anspruch auf Auszahlung des Guthabens der Erben gegenüber einer Bank haben Erben gegenüber dem Anbieter den Anspruch auf Zugriff auf die auf seinen Servern gespeicherten Daten.[130]

Urheberrechtlich geschützte eigene Inhalte

Soweit die eigenen Inhalte urheberrechtlichen Schutz genießen, d. h. es sich dabei um ein Werk[131] der Literatur, Wissenschaft oder Kunst handelt (vgl. § 1 UrhG), sind diese vererblich (vgl. § 28 I UrhG).[132] Dabei kann es sich u. a. um Grafiken, Texte, auch Briefe und Tagebücher, Fotografien[133] oder auch selbst komponierte Musik handeln. Auf den Erben gehen grundsätzlich sämtliche Urheberrechte des Erblassers über, sowohl die persönlichkeitsrechtlichen (vgl. §§ 12 ff. UrhG) als auch die vermögensrechtlichen (vgl. §§ 15 ff. UrhG).

Postmortales Persönlichkeitsrecht

Das allgemeine Persönlichkeitsrecht des Erblassers bleibt nach seinem Tod eingeschränkt in seiner Ausprägung als postmortales Persönlichkeitsrecht erhalten. Seine vermögensrechtlichen Bestandteile (wie das Recht am eigenen Bild) gehen gemäß § 1922 BGB auf die Erben über.[134] Der BGH hat im Facebook-Urteil dargelegt, dass vermögensrechtliche Rechtspositionen regelmäßig vererbt werden

[128] Stieper, ZUM 2019, S. 1 (4).

[129] Für vorstehenden Absatz: *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn. 14, mit Verweis auf *BGH*, GRUR 2016, 109; siehe *Stieper*, ZUM 2019, 1 (3).

[130] *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn. 25.

[131] § 2 UrhG enthält Beispiele für infrage kommender Werkkategorien.

[132] Der Urheber kann durch letztwillige Verfügung die Ausübung des Urheberrechts einem Testamentsvollstrecker übertragen (vgl. 28 II UrhG).

[133] Erreichen Fotos nicht die Gestaltungshöhe, um als Lichtbildwerk zu gelten, können sie gemäß § 72 UrhG als Lichtbilder und Erzeugnisse, die ähnlich wie Lichtbilder hergestellt werden, geschützt sein.

[134] Das Recht am eigenen Bild ist in § 22 KUG geregelt. Die Schutzdauer der vermögenswerten Bestandteile des postmortalen Persönlichkeitsrechts ist auf zehn Jahre nach dem Tod der Person begrenzt (vgl. § 22 S. 3 KUG). Auf den Erben gehen Vermarktungsrechte, Abwehr und Schadensersatzansprüche über.

können, auch wenn sie persönlichkeitsbezogene Elemente beinhalten. Als Wahrnehmungsberechtigte für die ideellen Anteile des postmortalen Persönlichkeitsrechts haben die nächsten Angehörigen (vgl. § 22 S. 4 KUG, § 77 II StGB) Abwehrrechte, z. B. wenn der gute Ruf des Verstorbenen beschädigt wird. Diese können sie bei einem Eingriff auch gegenüber den Erben ausüben, (bei denen es sich nicht zwangsläufig um nächste Angehörige handeln muss). Der Senat stellte fest, dass dies aber „ein dem Erbrecht vorgehendes Recht der nächsten Angehörigen an den höchstpersönlichen digitalen Inhalten nicht begründet“.[135]

5.3.4.3 Cloud beim Downloadanbieter

Die Rechte des Erblassers an diesem Vertrag gehen gemäß § 1922 BGB auf den Erben über. Soweit Nutzungsverträge nicht nach § 399 BGB als höchstpersönlich anzusehen sind, gehen auch Lizenzverträge zu online veröffentlichten Werken oder Online-Abonnement-Verträge auf die Erben über.[136] Grundsätzlich kann das Nutzungsrecht auch zeitlich beschränkt eingeräumt werden (vgl. 31 I S. 2 UrhG).

Einräumung eines zeitlich begrenzten Nutzungsrechts

Ist das Nutzungsrecht bzw. Zugriffsrecht des Erblassers auf die Inhalte wirksam zeitlich begrenzt, geht das Vertragsverhältnis so auf die Erben über.[137] Auch Downloads müssen somit nicht zwingend mit der Hardware, auf der sie gespeichert sind, auf die Erben übergehen.[138]

Die Vererbung des Nutzungsrechts an einem urheberrechtlich geschützten Werk fällt nicht unter die zustimmungsbedürftige Übertragung gemäß § 34 UrhG.[139] Folglich ist das Nutzungsrecht ohne Zustimmung des Urhebers vererblich.[140]

Ist das Nutzungsrecht durch Vereinbarung mit dem Erblasser wirksam auf dessen Lebenszeit beschränkt, könnte der Anbieter dadurch den Übergang der Inhalte an die Erben verhindern.[141] Die Rechtsposition des Erblassers wäre in diesem Fall einem Nießbrauch ähnlich und würde mit seinem Tod untergehen.[142]

Voraussetzungen für die zeitliche Beschränkung des Nutzungsrechts ist, dass eine entsprechend formulierte Klausel wirksam in die AGB einbezogen wurde und der Kontrolle der §§ 305 ff. standhält.

Handelt es sich für den Nutzer erkennbar um ein mietähnliches Verhältnis, bei dem etwa gegen monatliche Zahlungen auf ein bestimmtes Kontingent an Musik, Hörbüchern oder sonstigen Inhalten

[135] *BGH*, NJW 2018, S. 3178 (3191) Rn. 53.
[136] *Raude*, RNotZ 2017, S. 17 (25).
[137] *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn 31.
[138] *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn 21.
[139] *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn 31.
[140] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn 22.
[141] *Herzog/Pruns*, in: Der digitale Nachlass, § 4 Rn 30.
[142] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn 22.

zugegriffen werden kann, sind entsprechende Klauseln nicht überraschend (z. B. bei Streamingdiensten).[143]

Wird beim Nutzer dagegen der Eindruck erweckt, dass er die Inhalte käuflich erwirbt, etwa durch einen Button „Jetzt Kaufen“, den er anklicken muss, stellt die zeitliche Beschränkung eine überraschende Klausel dar.[144]

5.4 Allgemeine Geschäftsbedingungen in der Kritik

Wie oben beschrieben werden AGB von dem Unternehmen, das beispielsweise einen Dienst über das Internet anbietet, vorformuliert und von dem Verbraucher i. d. R. (mindestens) im Rahmen der Erstanmeldung bei dem Dienst bestätigt. Dies bildet die Grundlage für die Geltung der AGB zwischen dem Dienstanbieter und dem Dienstnutzer. Der Verbraucher als Dienstnutzer kann i. d. R. keinen Einfluss auf die Inhalte der AGB nehmen. Selbst wenn er mit einer oder mehreren der AGB-Klauseln nicht einverstanden wäre, so hätte er lediglich die Wahl, den Dienst zu den in den AGB stehenden Bedingungen zu nutzen oder sich einen alternativen Dienst bzw. Dienstanbieter zu suchen. Der Dienstanbieter befindet sich gegenüber dem Dienstnutzer daher regelmäßig in einer sehr starken Position. Dies bedeutet jedoch nicht, dass der Verbraucher dem Dienstanbieter schutzlos ausgeliefert ist: Sowohl die wirksame Einbeziehung als auch die Wirksamkeit der AGB-Klauseln selbst müssen sich an den §§ 305 ff. BGB messen lassen.

Diese Bestimmungen des BGB schützen die Verbraucher z. B. vor AGB-Klauseln, die nach dem äußeren Erscheinungsbild des Vertrags so ungewöhnlich sind, dass der Verbraucher nicht mit ihnen zu rechnen braucht. Solche Klauseln werden daher nicht Bestandteil des Vertrags zwischen dem Dienstanbieter und dem Dienstnutzer.[145] Auch werden Verbraucher u. a. vor kurzfristigen Preiserhöhungen geschützt, die ggf. in den AGB geregelt werden sollen, sofern sich die Erhöhung des Entgelts auf Waren oder Leistungen bezieht, die innerhalb von vier Monaten nach Vertragsschluss geliefert oder erbracht werden sollen und es sich hierbei nicht um ein Dauerschuldverhältnis handelt. Solche Klauseln sind unwirksam. Ein weiteres Beispiel einer unwirksamen AGB-Klausel wäre eine Bestimmung, die den Verbraucher dahingehend beschränkt, dass er seine Ansprüche gegen den Dienstanbieter nur gerichtlich geltend machen darf, nachdem er eine gütliche Einigung in einem Verfahren zur außergerichtlichen Streitbeilegung versucht hat.

Im Folgenden werden die in Kapitel 5.2 auf Seite 117 dargestellten AGB-Klauseln nach Maßgaben der §§ 305 ff. BGB bewertet. Begonnen wird mit der Bewertung der wirksamen Einbeziehung der AGB.

[143] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn 24.

[144] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn 25.

[145] Ein Beispiel hierfür wäre, dass der Verbraucher in einem Ladengeschäft einen Staubsauger erwirbt. Regelt der Verkäufer in seinen AGB, dass bei jedem Staubsaugerkauf automatisch ein jährlicher Wartungsvertrag auf Kosten des Käufers abgeschlossen wird, ist diese AGB-Klausel aus Sicht des Verbrauchers – also des Käufers des Staubsaugers – überraschend. Die Klausel wird daher nicht Bestandteil des Vertrages zwischen dem Verkäufer und dem Verbraucher.

5.4.1 Wirksame Einbeziehung von AGB

Vor der Prüfung einzelner Klauseln von Allgemeinen Geschäftsbedingungen ist zu prüfen, ob diese überhaupt wirksam in den Vertrag einbezogen wurden. Damit die vom Anbieter gestellten Nutzungsbedingungen wirksam in den Vertrag einbezogen werden, sind die Voraussetzungen der §§ 305 ff BGB zu erfüllen.

Gemäß § 305 II BGB werden AGB u. a. nur dann wirksamer Vertragsbestandteil, wenn der Online-Anbieter bei Vertragsschluss ausdrücklich auf sie hinweist (§ 305 II Nr. 1 BGB), er dem Kunden die Möglichkeit verschafft, in zumutbarer Weise von ihrem Inhalt Kenntnis zu nehmen (§ 305 II Nr. 2 BGB), und wenn der Kunde mit ihrer Geltung einverstanden ist.

Weist ein Online-Anbieter auf der Bestellmaske deutlich und in der Nähe der eigentlichen Bestellung auf die AGB hin, entspricht dies der Anforderung des ausdrücklichen Hinweises gemäß § 305 II Nr. 1 BGB.[146] Die Kenntnisverschaffung kann durch einen gut sichtbaren Link, unter dem die AGB aufgerufen und ausgedruckt werden können, erfolgen. Der Link muss im Bestellverlauf zwangsweise passiert werden.[147]

Regelungen, die nicht in den AGB erwähnt werden, sondern beispielsweise nur in den FAQ, werden nicht wirksam in den Vertrag einbezogen.[148] Dies stellte der BGH im Facebook-Urteil hinsichtlich der Regelungen zum Gedenkzustand, die sich nur im Hilfebereich von Facebook befanden, fest.[149] Entsprechende Informationen der Anbieter sind zu Informationszwecken über den Umgang der Anbieter mit Todesfällen nachstehend unter „Andere Hinweise bezüglich des Todesfalls des Kontoinhabers“ zu finden.

Neben den Vorschriften des BGB zu Allgemeinen Geschäftsbedingungen können sich aus Spezialnormen weitere Anforderungen ergeben, etwa aus den Bestimmungen zu Fernabsatzverträgen[150] und zum elektronischen Geschäftsverkehr.[151] So hat der Online-Anbieter dem Kunden gemäß § 312i Nr. 4 BGB die Möglichkeit zu verschaffen, die Vertragsbestimmungen einschließlich der Allgemeinen Geschäftsbedingungen bei Vertragsschluss abzurufen und in wiedergabefähiger Form auf einem Datenträger zu speichern. Dies kann durch Einräumung einer Möglichkeit zum Download bzw. Abrufmöglichkeit der AGB per E-Mail erfolgen.[152]

Die zumutbare Möglichkeit der Kenntnisnahme gemäß § 305 II Nr. 2 BGB setzt voraus, dass die AGB lesbar und verständlich sind. Dies ist der Fall, wenn der „normal informierte, angemessen aufmerksame Durchschnittsverbraucher“[153] sie ohne juristische Vorbildung bzw. ohne Einholung eines Rechtsrats verstehen kann.[154] Ein Verständlichkeitsgebot auf europarechtlicher Ebene enthält Art. 5

[146] *Schwab*, AGB-Recht, S. 57, Rn. 34.
[147] *Föhlisch*, in: *Hoeren/Sieber/Holznagel*, Multimedia-Recht, AGB-Recht, Rn. 115.
[148] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 19 f.
[149] *BGH*, NJW 2018, 3178, S. 3180.
[150] §§ 312c ff. BGB.
[151] §§ 312i, 312j BGB.
[152] *Schirmbacher*, BGB § 312i, in: *Spindler/Schuster*, Recht der elektronischen Medien, Rn. 59 f.
[153] *EuGH*, Urteil vom 30.04.2014 – C-26/13.
[154] *Schwab*, AGB-Recht, S. 64, Rn. 58.

der „Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen“.[155] Gemäß Satz 1 müssen schriftliche AGB-Klauseln stets klar und verständlich abgefasst sein. Bei Zweifeln über die Bedeutung einer Klausel gilt gemäß S. 2 die für Verbraucher günstigste Auslegung. Hinsichtlich der Prüfung auf Verständlichkeit sind die nachfolgend genannten Vorschriften des BGB richtlinienkonform auszulegen.[156]

Abzugrenzen ist das Transparenzgebot des § 305 II Nr. 2 BGB von dem Transparenzgebot des § 307 I S. 2 BGB, welches im Rahmen der Inhaltskontrolle zu prüfen ist,[157] wenn auch die Übergänge fließend sein können.[158] Zur groben Unterscheidung kann man sagen, dass erstgenanntes Gebot einen sinnvollen Inhalt und ein Mindestmaß an Übersichtlichkeit fordert, damit die Klauseln wirksam in den Vertrag einbezogen werden. Nach letztgenanntem Gebot sind Klauseln unwirksam, die es dem Kunden erschweren, das Ausmaß seiner Rechte und Pflichten bzw. wirtschaftlichen Nachteile zu erkennen, insbesondere durch Verwendung von (juristischen) Fachbegriffen.[159]

Auch der Umfang der AGB muss vertretbar sein, damit sie wirksam einbezogen werden.[160] Im Folgenden erfolgen daher Anmerkungen zur Verständlichkeit, Übersichtlichkeit und Umfang in AGB anhand einzelner Beispiele,[161] ebenso die Übersichtlichkeit.[162]

Schon 2012 beanstandete der Verbraucherzentrale Bundesverband die Länge der AGB verschiedener Anbieter. Eine entsprechend eingereichte Klage des Verbraucherzentrale Bundesverbands gegen die AGB von Apple iTunes wurde aber nicht in der Sache entschieden, sondern vom Landgericht Berlin und der Berufungsinstanz mit der Begründung abgewiesen, dass die fehlende Einbeziehung der AGB nicht im Verbandsklageverfahren geltend gemacht werden könne.[163] Der Kläger hielt die Vertragsbedingungen von 21 DIN A4-Seiten für zu lang, außerdem seien sie fast ohne Nummerierung sowie in Schriftgröße 9 zu klein gehalten. Dies verhindere, dass Verbraucher die AGB in vollem Umfang wahrnehmen und begreifen könnten. Zudem wurde die Vermischung der Regelungen für verschiedene Vertragsabschlüsse moniert.[164]

Die Schrift der sogenannten „Bedingungen der Apple-Mediaservices“ ist inzwischen größer geworden, einschließlich der Datenschutzerklärung dürften sie im Umfang aber kaum abgenommen haben. Ob an der Gliederung und Übersichtlichkeit seit 2012 etwas verbessert wurde, kann hier nicht nachvollzogen werden, da die AGB von 2012 nicht vorliegen.

Die Verständlichkeit von Nutzungsbedingungen wird auch beeinträchtigt, wenn der ursprüngliche Text zwar in die Landessprache des Kunden übersetzt wurde, aber die Übersetzung zu allgemein gehalten

[155] Richtlinie 93/13/EWG vom 05.04.1993
[156] *Schwab*, AGB-Recht, S. 65, Rn. 60.
[157] Siehe diesbezüglich das nachfolgende Kapitel 5.4.2 auf der nächsten Seite.
[158] *Niebling*, in: *Niebling*, AGB-Recht, § 305, Rn. 92 f.
[159] *Schwab*, AGB-Recht, S. 564, Rn. 59 f.
[160] *Niebling*, in: *Niebling*, AGB-Recht, § 305, Rn. 91
[161] *Niebling*, in: *Niebling*, AGB-Recht, § 305, Rn. 91.
[162] *Schwab*, AGB-Recht, S. 66, Rn. 62.
[163] *Kammergericht Berlin*, Beschluss vom 17.10.2016 – 23 U 277/12.
[164] Information des VZBV, https://www.vzbv.de/urteil/klage-gegen-ueberlange-geschaeftsbedingungen-von-itunes-abgewiesen.

ist. So ist zum Beispiel in den iTunes-AGB nicht ohne Weiteres erkennbar, welche Apple-Tochter überhaupt der Vertragspartner der deutschen iTunes-Kunden ist. Dies muss der Kunde durch Ausschlussverfahren im Abschnitt „Definition von Apple“ herausfinden, wo an unterster Stelle Deutschland im folgenden Absatz nicht explizit erwähnt wird: „Apple Distribution International, mit Sitz in Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland für alle anderen Benutzer.“[165] Durch vorhergehende Formulierungen in verschiedenen Abschnitten der AGB wie, „Wenn Sie jedoch ein Kunde von Apple Distribution International sind. . . “, wird zudem der Eindruck erweckt, dass dies nicht die einzige Konzerntochter ist, die zum Vertragspartner des deutschen iTunes-Kunden wird.[166]

Fraglich ist auch, ob der Umfang der AGB von Amazon Kindle den durchschnittlichen Verbraucher nicht überfordert und noch vertretbar ist. Denn auf der Seite „Nutzungsbedingungen für Kindle eReader und Fire Tablets“[167] sind zahlreiche Links zu Nutzungsbedingungen aufgeführt, die der Kunde gegebenenfalls zu beachten hat. Unter dem Satz, „mit Ihrer Bestellung oder der Registrierung eines Kindle eReaders, Fire Tablets, einer Kindle Lese-App oder der Amazon App Suite erklären Sie sich mit den folgenden zusätzlichen Bedingungen einverstanden“, folgen zunächst sechs Links zu verschiedenen Nutzungsbedingungen.[168] Je nachdem, ob der Kunde eine Bestellung über Amazon Prime, Amazon oder FreeTime Unlimited oder Kindle Unlimited über seinen Kindle eReader, Fire Tablet oder eine Lese-App tätigt, stimmt er laut Amazon außerdem den folgenden Bedingungen zu: Amazon Prime: Teilnahmebedingungen, FreeTime Unlimited – Nutzungsbedingungen oder Kindle Unlimited Nutzungsbedingungen. Die verschiedenen Nutzungsbedingungen beinhalten dann wiederum aufeinander verweisende Links, worunter die Übersichtlichkeit leidet.[169]

Vorgenannte Beispiele aus den AGB sind nicht abschließend und sollen vor allem beleuchten, dass Verbraucherschutz nicht nur die expliziten Regelungen zum Nachlass bzw. Recht an digitalen Gütern betrifft. Sie sollen und können die Frage der wirksamen Einbeziehung nicht abschließend klären.

5.4.2 Wirksamkeit der AGB

Wurden AGB wirksam einbezogen, ist darauf folgend zu prüfen, ob die einzelnen Klauseln (selbst) wirksam sind. Zweifel bei der Auslegung von AGB gehen hierbei regelmäßig zu Lasten des Verwenders. Ist eine Klausel zwar wirksam einbezogen, aber etwa missverständlich, mehrdeutig oder widersprüchlich, gilt die Deutung, die dem Kunden die weitgehendsten Rechte und wenigsten Pflichten einräumt.[170] In den nachfolgenden Unterkapiteln wird die Wirksamkeit der in Kapitel 5.2 auf Seite 117

[165] Bedingungen der Apple Media Services, beispielsweise Abschnitt K., Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html.

[166] Bedingungen der Apple Media Services, beispielsweise Abschnitt B., Stand 13.05.2019, https://www.apple.com/legal/internet-services/itunes/de/terms.html.

[167] Diese ist abrufbar unter https://www.amazon.de/gp/help/customer/display.html?nodeId=200144520.

[168] Die o. g. sechs Links führen zu den Nutzungsbedingungen für den Kindle-Shop, Amazon.de Allgemeine Geschäftsbedingungen, Nutzungsbedingungen für Amazon-Geräte, Amazon Drive und Prime Photos Nutzungsbedingungen, Audible.de Allgemeine Geschäftsbedingungen, Alexa Nutzungsbedingungen.

[169] Siehe dazu auch Kapitel 5.2.4.1 auf Seite 122.

[170] *Schwab*, AGB-Recht, S. 65, Rn. 59 f., *Niebling*, in: *Niebling*, AGB-Recht, § 305, Rn. 93.

vorgestellten AGB anhand von Fallgruppen untersucht, um alle relevanten Prüfaspekte thematisch sortiert diskutieren zu können.

5.4.2.1 Benennung der kostenpflichtigen Aktivität und Beschränkung der Lizenz

I. d. R. erwirbt der Dienstnutzer für digitale Werte wie z. B. Film-, Musik- und Buchdateien eine nicht-exklusive und nicht-übertragbare Lizenz zur privaten Nutzung. Die kommerzielle Nutzung, Verbreitung, Vermietung und der Weiterverkauf sind i. d. R. ausgeschlossen. Obwohl die meisten der untersuchten Dienstanbieter in ihren AGB deutlich betonen, dass der Dienstnutzer lediglich eine Lizenz erwirbt und der digitale Wert somit nicht in sein Eigentum übergeht, verwenden einige Anbieter trotzdem auch den Begriff „Kaufen“. So unterscheiden einige Dienstanbieter etwa zwischen dem „Kauf“ und der „Miete“, wobei ein gemieteter digitaler Wert im Gegensatz zum gekauften digitalen Wert nur für einen im Vorfeld definierten Zeitraum (z. B. 30 Tage nach Zahlung) zur Verfügung steht.

Die Frage, ob der Erschöpfungsgrundsatz – siehe Kapitel 5.3.3 auf Seite 134 – auch für im Rahmen von Online-Downloads erworbene Film-, Musik-, Spiel- und Buchdateien gilt, ist umstritten. Die herrschende Meinung in Rechtsprechung und Literatur spricht sich jedoch dagegen aus, sodass etwa nach der Rechtsprechung des OLG Hamburg[171] und des OLG Hamm[172] AGB-Klauseln, die die Weiterveräußerung digitaler Güter (wie E-Books und Hörbücher bzw. Audiodateien) verbieten, keine unangemessene Benachteiligung gemäß § 307 BGB besteht.[173] Des Weiteren entschied das OLG Hamm, dass in den Allgemeinen Geschäftsbedingungen eines Anbieters zu Hörbüchern, die von Kunden heruntergeladen und auf eigenen Datenträgern gespeichert werden, nicht zu beanstanden ist, wenn der Kunde ein einfaches, nicht übertragbares Recht erhält, „die angebotenen Titel zum ausschließlich persönlichen Gebrauch gemäß Urheberrechtsgesetz in der jeweils angebotenen Art und Weise zu nutzen“ und dem Kunden untersagt wird, die Dateien für Dritte zu kopieren oder weiterzuverkaufen.[174]

Zu beachten ist jedoch, dass eine *zeitliche Beschränkung des Nutzungsrechts* durch die AGB des Dienstanbieters regelmäßig nur dann wirksam ist, wenn sie nicht überraschend ist. Überraschend – und somit unwirksam – wäre es regelmäßig, wenn beim Nutzer der Eindruck erweckt wird, dass er die Inhalte käuflich erwirbt, etwa durch einen Button, „Jetzt Kaufen“, den er anklicken muss.[175] Für weiterführende Informationen wird auf die detaillierte Darstellung in Kapitel 5.3.3 auf Seite 134 verwiesen.

Einer der untersuchten Anbieter, Apple für Apple iTunes, regelt darüber hinaus explizit, dass sofern gesetzlich nichts anderes vorgeschrieben ist, der Account des Dienstnutzers nicht übertragbar ist und dass alle Rechte an den digitalen Werten, die mit dem Account in Verbindung stehen, im Todesfall des Dienstnutzers enden. Diesbezüglich wird ebenfalls auf die Ausführungen aus Kapitel 5.3.3 auf Seite 134 – insbesondere auch auf Kapitel 5.3.4.3 auf Seite 144 – verwiesen.

[171] *OLG Hamburg*, ZUM 2015, S. 503.
[172] *OLG Hamm*, NJW 2014, S. 3659.
[173] Zum Meinungsstand in Rechtsprechung und Literatur, Heerma, in: Wandtke/Bullinger, UrhG, § 17, Rn. 30.
[174] *OLG Hamm*, NJW 2014, S. 3659.
[175] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 24 f.

5.4.2.2 Übertragbarkeit des Nutzerkontos

Regelungen, die dem Nutzer die Übertragung des Nutzerkontos oder die Weitergabe des Passworts an Dritte untersagen, beziehen sich in der Regel auf das Verhalten zu Lebzeiten des Nutzers und enthalten keine Aussagen für den Todesfall bzw. die Vererbarkeit.[176] Erben sind auch infolge der Universalsukzession keine Dritten, denen kein Zugang verschafft werden dürfte.[177]

Wie der BGH im Facebook-Urteil erklärte, geht nach § 1922 I BGB das Vermögen als Ganzes auf die Erben über, wozu grundsätzlich auch Ansprüche und Verbindlichkeiten aus schuldrechtlichen Verträgen respektive Online-Nutzungsverträgen zählen.[178] Der Anspruch auf den Zugang zu einem Nutzerkonto ergibt sich aus dem Übergang des Vertragsverhältnisses auf die Erben. Die Vererbbarkeit von Ansprüchen könne zwar vertraglich ausgeschlossen werden; die Frage, ob die Vererbbarkeit des vertraglichen Nutzungsverhältnisses und des daraus folgenden Kontozugangsrechts in AGB grundsätzlich wirksam ausgeschlossen werden kann, ließ der BGH aber offen.[179] Ein genereller Ausschluss der Vererblichkeit eines Nutzerkontos in AGB wird in der Literatur überwiegend für unwirksam erachtet, da dies an § 307 BGB scheitert. [180]

Bezüglich Social-Network-Konten (wie Facebook) befand der BGH, dass der aus dem Nutzungsvertrag folgende Anspruch auf Zugang weder wirksam durch die AGB ausgeschlossen wurde, noch ließe sich ein Ausschluss der Vererbbarkeit aus dem Wesen des Vertrags ableiten – wie das etwa bei Verträgen, die eine höchstpersönliche Leistungserbringung beinhalten, der Fall ist (etwa der Partnervermittlung oder ärztlichen Behandlung).[181] Zwar sei das Vertragsverhältnis insoweit personenbezogen, als nur der Kontoinhaber (hier Erblasser) Inhalte veröffentlichen und Nachrichten schreiben dürfe, dies führe aber nicht zur Unvererbbarkeit, sondern könnte allenfalls dazu führen, dass die aktive Weiternutzung durch den Erben nicht von seinem Erbrecht umfasst ist – wie beim Girovertrag.[182]

Die Leistungen seien bei jedem Nutzer gleich. Facebook verpflichte sich, die Kommunikationsplattform zur Verfügung zu stellen und entsprechend dem Auftrag des Nutzers Inhalte zu veröffentlichen oder Nachrichten an ein anderes Benutzerkonto zu übermitteln sowie übermittelte Nachrichten bzw. geteilte Inhalte zugänglich zu machen.[183] Nur die – von der Vertragsgestaltung unabhängigen – Inhalte, die von Nutzern geschaffen und kommuniziert werden, seien persönlichkeitsrelevant.

Ausweitung auf weitere Online-Dienste

Das LG Münster hat die Rechtsprechung des BGH auf weitere Online-Dienste ausgedehnt, es verurteilte Apple dazu, den Erben Zugang zu dem vollständigen Benutzerkonto in der iCloud und den darin vorgehaltenen Inhalten des Erblassers zu gewähren. Mit Verweis auf das Facebook-Urteil stellte das

[176] Herzog/Pruns in: Der digitale Nachlass, § 5 Rn. 13; BGH, NJW 2018, 3178 (3180) Rn. 25.
[177] Für vorstehenden Absatz: Herzog/Pruns in: Der digitale Nachlass, § 5, Rn. 13.
[178] Siehe dazu Kapitel 2 auf Seite 35.
[179] *BGH*, NJW 2018, S. 3178 (3180) Rn. 18–25.
[180] Für vorstehenden Absatz: *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 31, mit weiteren Verweisen *Gomille*, ZUM 2018, 660 (667).
[181] *BGH*, NJW 2018, S. 3178 (3180) Rn. 23.
[182] *BGH*, NJW 2018, S. 3178 (3181) Rn. 36.
[183] *BGH*, NJW 2018, S. 3178 (3181) Rn. 33 ff.

LG fest, der Anspruch sei gemäß § 1922 BGB i. V. m. dem Nutzungsvertrag vererblich und weder das postmortale Persönlichkeitsrecht noch andere Rechte stünden ihm entgegen.[184]

Folgen für Vorsorgebevollmächtigte und Betreuer

Da sich – wie oben erwähnt – Regelungen, die dem Nutzer die Übertragung des Nutzerkontos oder die Weitergabe des Passworts an Dritte untersagen, in der Regel auf das Verhalten zu Lebzeiten des Nutzers beziehen, stellt sich auch die Frage der Zulässigkeit solcher Klauseln in Bezug auf Zugriffsmöglichkeiten durch einen Vorsorgebevollmächtigten oder einen Betreuer.

Hierbei wird es zunächst darauf ankommen, ob ein Vorsorgebevollmächtigter oder Betreuer als „Dritter“ zu verstehen ist, an den laut der jeweiligen AGB-Klausel keine Übertragung des Nutzerkontos erfolgen darf und/oder an den die Weitergabe des Passworts untersagt ist. Eine Definition des Begriffs „Dritter“ in den AGB der jeweiligen Anbieter erfolgt nicht.[185] Es ist jedoch davon auszugehen, dass Vorsorgebevollmächtigte und Betreuer keine Dritten i. S. d. Klausel sind, da die Nutzung der Dienste durch Betreuer und Vorsorgebevollmächtigte gerade die sichere Nutzung durch den Betreuten sicherstellen bzw. ihm eine Hilfe bieten soll.

Selbst wenn Vorsorgebevollmächtigte und Betreuer aber „Dritte“ im Sinne der betroffenen AGB-Klauseln sein sollten, wären solche AGB-Klauseln wohl regelmäßig als unwirksam i. S. d. § 307 II Nr. 1 BGB einzustufen.[186]

Dies ergibt sich für Vorsorgebevollmächtige aus der Unvereinbarkeit solcher Klauseln mit dem Willen des Gesetzgebers, die private Vorsorge für den Fall der Handlungsunfähigkeit zu ermöglichen und zu fördern – könnte eine AGB-Klausel ein mögliches Handeln eines Vorsorgebevollmächtigten ausschließen, wäre die Möglichkeit der privaten Vorsorge erheblich beschränkt und für den digitalen Bereich nahezu unmöglich. Für Betreuer ergibt sich dies wiederum aus dem Umstand, dass durch die Anordnung einer Betreuung sichergestellt werden soll, die Handlungsfähigkeit des Betreuten so lange wie möglich aufrechterhalten zu können. Sofern der Betreuer aber im digitalen Bereich nicht für den Betreuten tätig werden kann, verträgt sich dies ebenfalls regelmäßig nicht mit dem Willen des Gesetzgebers.

5.4.2.3 Gedenkzustand

Ungeachtet dessen, dass die Regelungen zum Gedenkzustand (gemäß § 305 II BGB) nicht wirksam einbezogen wurden, stellte der BGH fest, dass diese auch einer Inhaltskontrolle nach Maßgabe von § 307 I, II Nr. 1 BGB nicht standhalten würden. Die Regelungen schlössen zwar die Vererbung des Nutzungsverhältnisses nicht als solches aus, führten aber zu dessen Aushöhlung, indem sie nachträglich die Leistungspflichten von Facebook veränderten. Nach Mitteilung des Todesfalls durch einen beliebigen Dritten werde den Erben das Zugangsrecht zu dem Konto verwehrt und damit ein

[184] *LG Münster*, K & R 2019, S. 422.

[185] Vgl. hierzu insbesondere die AGB von PayPal und Facebook.

[186] Hierzu analog: *Herzog/Pruns*, in: Der digitale Nachlass, § 5, Rn. 31, mit weiteren Verweisen; *Gomille*, ZUM 2018, 660 (667).

Hauptleistungsanspruch. Angesichts der erheblichen Einschränkung der vertraglichen Rechte der in den Nutzungsvertrag eingetretenen Erben, liege eine unangemessene Benachteiligung im Sinne von § 307 I, II BGB vor. Dies widerspreche den wesentlichen Grundgedanken des § 1922 BGB, der den Übergang eines Schuldverhältnisses mit allen Rechten und Pflichten auf den Erben vorsieht.[187]

Dass durch den Gedenkzustand die Erreichung des Vertragszwecks nicht mehr möglich ist, weil die wesentlichen Rechte aus dem Vertragsverhältnis entfallen, nämlich der Zugang zum Benutzerkonto, der Zugriff auf dort gespeicherte Inhalte und die Verfügungsbefugnis darüber, wertete der BGH gleichzeitig als Verstoß gegen § 307 II Nr. 2 BGB.[188]

5.4.2.4 Nachlasskontakt

Das erstinstanzliche „Facebook-Urteil“ des Landgerichts Berlin erging 2015. Inzwischen hat Facebook seine AGB überarbeitet, die Gedenkzustand-Funktion aber beibehalten (siehe dazu oben). Hinzugefügt worden ist die Möglichkeit, einen Nachlasskontakt anzugeben. Ein Internet-Link in der Klausel zum Nachlasskontakt verweist nun auf die Erläuterungen im Hilfebereich. Dies könnte zumindest der Einbeziehung gemäß § 305 BGB genügen.[189]

Dennoch bleibt zweifelhaft, ob die Einbindung eines Nachlasskontakts, so wie Facebook dies vorsieht, rechtskonform ausgestaltet wurde. So scheint es dem Dienstnutzer insbesondere nicht möglich, wirklich frei zu entscheiden, was nach seinem Tod mit seinem Nutzeraccount passieren soll. Die von Facebook zugestandene Wahlmöglichkeit, genau *einen* Nachlasskontakt – bei dem es sich *zwingend* um einen anderen Facebook-Nutzer handeln muss – zu benennen oder nicht, bilden jedenfalls zumindest nicht die aus erbrechtlicher Sicht bestehenden Wahlmöglichkeiten des Dienstnutzers ab.

5.4.2.5 Inaktivität

Klauseln bezüglich der Deaktivierung von Nutzer-Accounts, die für einen längeren Zeitraum nicht genutzt wurden, dürften grundsätzlich zulässig sein, wenn die Inaktivitätszeit nicht zu kurz bemessen ist und der Nutzer vor der Deaktivierung informiert wurde. Ansonsten müssten die Anbieter die Belastung durch eine Vielzahl verwaister Accounts hinnehmen.[190]

Diese Einschätzung ist auch zu teilen, wenn mit der Deaktivierung des Accounts der Verfall eines Guthabens einhergeht, sofern auch hier die Inaktivität nicht zu kurz bemessen ist[191] und der Dienstnutzer rechtzeitig über die bevorstehende Deaktivierung informiert wird und den Guthabenverfall durch eine einmalige Handlung – also die Reaktivierung des Accounts durch einen erneuten Login – verhindern

[187] *BGH*, NJW 2018, S. 3178 (3180) Rn. 28, 30.
[188] *BGH*, NJW 2018, S. 3178 (3180) Rn. 31.
[189] *Härting*, in: *Niebling*, AGB-Recht, Lexikon IT- und EDV-Verträge, Rn. 1198.
[190] Für vorstehenden Absatz: *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 14.
[191] z. B. wählen Sony PlayStation und PayPal einen Zeitraum von 24 bzw. 36 Monaten ohne Nutzeraktivität, bis eine Deaktivierung des Accounts erfolgt, was regelmäßig angemessen sein dürfte.

kann. Hierfür hat der Dienstanbieter dem Dienstnutzer einen angemessenen Reaktionszeitraum zu gewähren.

5.4.2.6 Guthabenübertragung, -rückerstattung und -gültigkeit

AGB-Klauseln, die den Ausschluss einer Guthabenübertragung an Dritte, den Ausschluss der Rückerstattung von erworbenem Guthaben und/oder die Gültigkeit des erworbenen Guthabens betreffen, sollten aufgrund ihrer besonderen Bedeutung für den Verbraucher grundsätzlich deutlich hervorgehoben werden. Ein „Verstecken“ solcher Klauseln in den i. d. R. langen AGB ohne weitere Hervorhebung erscheint intransparent, gleiches gilt für Formulierungen wie „[Rückerstattungen sind ausgeschlossen. Eine Ausnahme besteht,] wenn es gesetzlich erforderlich ist.“ Die Intransparenz kann jedoch in diesem Fall i. d. R. durch die Nennung konkreter Beispiele abgewandt werden.

Regelungen, die dem Nutzer die Übertragung des Guthabens untersagen, beziehen sich in der Regel auf das Verhalten zu Lebzeiten des Nutzers und enthalten keine Aussagen für den Todesfall bzw. die Vererbbarkeit.[192] Dies dürfte grundsätzlich auch auf Klauseln zutreffen, die das persönliche „Eigentum“ an erworbenem Guthaben ausschließen. Diesbezüglich wird für nähere Ausführungen auf Kapitel 5.4.2.2 auf Seite 150 verwiesen.

Potenziell kann auch eine zu kurze Gültigkeit eines vom Erblasser erworbenen Guthabens für seine Erben nachteilig wirken. Die Beschränkung eines Guthabenwerts auf 24 Monate erscheint aus Sicht des Erblassers überraschend – sodass entsprechende Klauseln ggf. nicht wirksam einbezogen würden – und stellt einen (potenziell) erheblichen wirtschaftlichen Nachteil des Erblassers und ggf. dessen Erben dar. Vergleicht man das zur Nutzung in einem Online-Dienst erworbene Guthaben mit einem Gutschein, so gilt für diesen grundsätzlich eine Gültigkeit von drei Jahren ab Ende des Jahres, in dem der Gutschein ausgestellt wurde, §§ 195, 199 BGB. Im Einzelfall kann von dieser Gültigkeit zwar abgewichen werden, die Rechtsprechung ist in Bezug auf die Gültigkeit von Gutscheinen jedoch nicht eindeutig, sodass im Ergebnis die Orientierung an §§ 195, 199 BGB zu empfehlen ist.

5.4.2.7 Koppelung der Erben an den Dienst

AGB-Klauseln sowie sonstige Bestimmungen der Dienstanbieter, welche die *Erben* an den vom Dienstanbieter angebotenen Dienst binden bzw. eine Benachteiligung derjenigen Erben darstellen, die nicht selbst Dienstnutzer sind, sind grundsätzlich bedenklich.

Insbesondere ist bedenklich, wenn der Dienstanbieter die Möglichkeit, einen Nachlasskontakt anzugeben, insofern beschränkt, als es sich bei der benannten Person zwingend um einen anderen Dienstnutzer handeln muss, weil dies die Wahlmöglichkeit des Dienstnutzers ggf. erheblich einschränken kann.

Auch Bearbeitungsgebühren, die nur diejenigen Erben treffen, die selbst keine Dienstnutzer sind, sind in diesem Zusammenhang zumindest als bedenklich – bzw. sofern sie den Regelungen der

[192] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 13; *BGH*, NJW 2018, 3178 (3180) Rn. 25

§§ 305 ff. BGB standhalten müssen – als überraschend einzustufen. In diesem Sinne wäre grundsätzlich auch die von PayPal[193] erhobene Gebühr von 40 US-Dollar bedenklich, die erhoben wird, wenn ein zurückzuerstattendes Guthaben nicht auf ein anderes PayPal-Konto überwiesen werden soll. Im konkreten Fall stellt jedoch die weitere Einschränkung, dass die Gebühr auch dann nicht erhoben wird, wenn das Guthaben auf das im Rahmen des Dienstes registrierte Bankkonto des Erblassers überwiesen werden soll, eine angemessene, die Erben als „Nicht-Dienstnutzer“ nicht benachteiligende Alternative dar.

5.4.3 Rechtsdurchsetzung

Sofern ein Verbraucher z. B. eine AGB-Klausel für unwirksam hält, bleibt dem Verbraucher zur Durchsetzung seiner Rechte zunächst die Option eines Zivilgerichtsverfahrens.

5.4.3.1 Zivilgerichtsverfahren

Dieses beginnt i. d. R. mit Erhebung der Klage – im Falle, dass ein Verbraucher seine Rechte gegenüber einem Dienstanbieter geltend machen möchte, also mit Klageerhebung durch den Verbraucher bzw. dessen Rechtsanwalt.[194] Mit der Klage ist ein Vorschuss auf die Gerichtskosten zu leisten, i. d. R. ist zudem ein Vorschuss an den ggf. beauftragten Rechtsanwalt zu leisten. Sofern der Verbraucher bedürftig ist, eine hinreichende Aussicht auf Erfolg besteht und die Klage nicht mutwillig erscheint, kann der Verbraucher ggf. Prozesskostenhilfe in Anspruch nehmen, §§ 114 ff. ZPO.

Das Gericht stellt die Klage sodann dem Beklagten – also dem Dienstanbieter – zu und verfügt über den weiteren Verlauf des Verfahrens, z. B. darüber, ob ein schriftliches Vorverfahren oder direkt eine mündliche Verhandlung erfolgen soll. Das Verfahren endet i. d. R. mit der Rücknahme der Klage durch den Kläger, durch die Anerkennung der Ansprüche des Klägers durch den Beklagten, durch einen zwischen Kläger und Beklagtem geschlossenen Vergleich[195] oder durch Urteil des Gerichts.

Gegen ein im ersten Rechtszug erlassenes Endurteil können sowohl der Kläger als auch der Beklagte das Rechtsmittel der Berufung einlegen, sofern der Wert des Beschwerdegegenstandes 600 Euro übersteigt oder das Gericht des ersten Rechtszuges die Berufung im Urteil zugelassen hat, § 511 ZPO. Über die Berufung entscheidet das zuständige Landgericht, wenn das Urteil im ersten Rechtszug durch ein Amtsgericht gesprochen wurde und nicht – wie beispielsweise in Familiensachen – das

[193] Auf die von PayPal erhobene Gebühr wird lediglich im Hilfe-Forum hingewiesen. Sie ist nicht Bestandteil der AGB von PayPal.

[194] Bei Klageerhebung vor einem Amtsgericht kann der Verbraucher i. d. R. auf die Vertretung durch einen Rechtsanwalt verzichten, sofern er dies möchte und sich zutraut, seine Ansprüche selbst durchzusetzen. Vor den Land- und Oberlandesgerichten besteht hingegen regelmäßig die Pflicht, sich durch einen Rechtsanwalt vertreten zu lassen, § 78 Zivilprozessordnung (ZPO). Ob in erster Instanz das Amts- oder Landgericht zuständig ist, entscheidet regelmäßig der Streitwert, wobei Amtsgerichte i. d. R. für einen Streitwert von bis zu 5.000 Euro zuständig sind, § 23 Gerichtsverfassungsgesetz (GVG).

[195] Bei einem Vergleich handelt es sich um eine Einigung im Wege *gegenseitigen* Nachgebens, auf die ein Gericht ausdrücklich bedacht sein soll, § 278 ZPO, § 779 BGB.

Oberlandesgericht zuständig ist, §§ 71 ff. GVG. Wurde das Urteil im ersten Rechtszug durch ein Landesgericht gesprochen, ist für die Berufung regelmäßig das Oberlandesgericht zuständig, siehe §§ 115 ff. GVG.

In Ausnahmefällen können der Kläger und der Beklagte darüber hinaus das Rechtsmittel der Revision einlegen, welche sich gegen das in der Berufungsinstanz erlassene Endurteil richtet. Die Revision findet jedoch nur statt, wenn sie das Berufungsgericht oder (auf Beschwerde der Nichtzulassung) das Revisionsgericht zulassen. Die Revision – die vor dem Oberlandesgericht bzw. dem Bundesgerichtshof erfolgt – ist regelmäßig nur dann zuzulassen, wenn die Rechtssache von grundsätzlicher Bedeutung ist oder die Rechtssache die Fortbildung des Rechts bzw. die Sicherung einer einheitlichen Rechtsprechung erfordert, § 543 ZPO.

Die Kosten eines Rechtsstreits trägt diejenige Partei, die im Rechtsstreit (endgültig) unterliegt. Sofern eine Partei nur teilweise unterliegt, werden die Kosten des Rechtsstreits entsprechend aufgeteilt. Sofern der Kläger im Laufe des Verfahrens seine Klage zurücknimmt, trägt er die Kosten des Rechtsstreits. Das gleiche gilt für den Beklagten, wenn dieser im Laufe des Verfahrens die Ansprüche des Klägers anerkennt. Sofern sich beide Parteien im Wege des gegenseitigen Nachgebens durch einen Vergleich einigen, tragen der Kläger und der Beklagte die Gerichtskosten je zur Hälfte, ihre Anwaltskosten sowie ggf. weitere außergerichtliche Kosten trägt jede Partei selbst. Ein Vergleich kann jedoch auch eine davon abweichende Regelung, auf die sich Kläger und Beklagter geeinigt haben, enthalten, §§ 91 ff. ZPO. Die Kosten eines Rechtsstreits ergeben sich insbesondere aus dem Gerichtskostengesetz (GKG) und dem Rechtsanwaltsvergütungsgesetz (RVG).

Zieht ein Verbraucher also gegen einen Dienstanbieter vor Gericht, so trägt er zunächst ein finanzielles Risiko in Bezug auf die Kosten des Rechtsstreits. Um die Kosten eines Rechtsstreits im Vorfeld abschätzen zu können, haben sich Services rund um die Berechnung der Prozesskosten entwickelt, wie z. B. der Prozesskostenrechner des Deutschen Anwaltsvereins.[196] Bei einem Streitwert von 800 Euro liegen die Kosten des Rechtsstreits – sofern sich diese nur aus den Gerichtskosten sowie den Anwälten des Klägers und des Beklagten zusammensetzen und nicht beispielsweise weitere Kosten für Gutachter anfallen – laut dem Prozesskostenrechner bei ca. 770 Euro bzw. 1.560 Euro (bei Berufung) bzw. 2.600 Euro (bei Revision). Bei einem Streitwert von 2.000 Euro liegen die Kosten des Rechtsstreits bereits bei ca. 1.350 Euro bzw. 2.750 Euro bzw. 4.600 Euro.

Hinzu kommt, dass sich Verfahren häufig über einen sehr langen Zeitraum ziehen, so gibt beispielsweise das Kammergericht Berlin die durchschnittliche Verfahrensdauer der Zivilsachen mit 14,6 Monaten an.[197] Es ist zu unterstellen, dass sowohl das potenziell sehr hohe finanzielle Risiko sowie die langen Zeiträume bis zu einer endgültigen Entscheidung den Verbraucher sehr stark belasten – insbesondere vor dem Hintergrund, dass den Verbrauchern bewusst sein dürfte, dass Unternehmen im Zweifelsfall über „den längeren Atem“ verfügen, was die finanziellen Mittel in Bezug auf das Einlegen von Rechtsmitteln angeht, was die Angst der Verbraucher, der Dienstanbieter könnte die endgültige Entscheidung über viele Monate oder sogar Jahre „verschleppen“, zusätzlich schüren dürfte. Auch

[196] Siehe unter https://anwaltverein.de/de/service/prozesskostenrechner.
[197] Siehe hierzu https://www.berlin.de/gerichte/kammergericht/das-gericht/wir-ueber-uns/statistik.

können sich Verbraucher durch diese Umstände unter Druck gesetzt fühlen, einen vom Dienstanbieter vorgeschlagenen Vergleich zu akzeptieren, um jahrelangen Streitigkeiten vor Gericht sowie dem damit verbundenen finanziellen Risiko aus dem Weg zu gehen. Dies wiederum stellt für diejenigen Verbraucher einen Nachteil dar, für die eine endgültige Entscheidung eines Gerichts – also z. B. darüber, dass eine AGB-Klausel unwirksam ist – eine gewisse Sicherheit wäre, ihre eigenen Ansprüche vor Gericht durchsetzen zu lassen. Vielfach wird auch die Geringfügigkeit eines dem Verbraucher entstandenen Schadens den Verbraucher davon abhalten, seine Ansprüche vor Gericht durchzusetzen.

5.4.3.2 Musterfeststellungsklage

Genau bei diesen Problemen setzt die sogenannte Musterfeststellungsklage an. Die Musterfeststellungsklage soll in einem durch Massengeschäfte geprägten Wirtschaftsleben unrechtmäßige Verhaltensweisen von Dienstanbietern, durch die eine Vielzahl gleichartig geschädigter Verbraucher entsteht, ihre Wirkung entfalten. Gerade dort, wo ein erlittener Schaden – oder allgemeiner formuliert: Nachteil – des Verbrauchers für den Einzelfall betrachtet gering ausfällt, werden Ansprüche des Verbrauchers i. d. R. nicht weiterverfolgt, da es sich aus Sicht des Verbrauchers um einen unverhältnismäßigen Aufwand handelt, die Ansprüche wie in Kapitel 5.4.3.1 auf Seite 154 beschrieben durchzusetzen. Sofern der Verbraucher seine Rechte jedoch nicht durchsetzt, verbleibt der unrechtmäßig erlangte Gewinn eines Dienstanbieters bei eben diesem. Auch soll die neue Musterfeststellungsklage – neben dem Problem des Desinteresses der Verfolgung geringfügiger Nachteile – auch darauf hinwirken, dass Verbraucher nicht vor der Ungewissheit der Rechtsprechung zurückschrecken.[198]

Die Musterfestellungsklage ist im „Gesetz zur Einführung einer zivilprozessualen Musterfeststellungsklage“ geregelt, welches am 1. November 2018 in Kraft getreten ist, und soll das Kräfteverhältnis zwischen den Verbrauchern und Dienstanbietern wiederherstellen. Das genannte Gesetz bewirkt u. a. Änderungen des Gerichtsverfassungsgesetzes und der Zivilprozessordnung.

Laut dem Bundesministerium der Justiz und für Verbraucherschutz können mithilfe der Musterfeststellungsklage „Unternehmen, die sich unrechtmäßig verhalten, einfacher und effektiver zur Verantwortung gezogen und die Ansprüche der Verbraucher leichter durchgesetzt werden.“[199] Grundlegendes Prinzip der Musterfeststellungsklage ist es, dass die Klage nicht durch einen Verbraucher selbst, sondern nur von Verbraucherschutzverbänden erhoben werden kann, § 606 I ZPO. Somit handelt es sich bei der Musterfeststellungsklage um eine Feststellungsklage im Drittinteresse.[200] Das Verfahren wird zwischen dem klagenden Verbraucherverband und dem beklagten Dienstanbieter geführt. In ihm werden alle Rechtsfragen geklärt, die für die Verbraucher im Rahmen ihrer ggf. bestehenden Ansprüche von Bedeutung sind. Um ihre Ansprüche im Rahmen der Musterfeststellungsklage durchzusetzen, müssen die Verbraucher ihre Ansprüche zunächst lediglich zum Klageregister anmelden, das vom

[198] *Waclawik*, NJW 2018, S. 2921 (2921).
[199] Siehe Pressemittelung des BMJV unter: https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2018/061418_MFK.html.
[200] *Waclawik*, NJW 2018, S. 2921 (2921).

Bundesamt für Justiz geführt wird.[201] Das Klageregister stellt somit die Verbindung zwischen der (von Dritten) erhobenen Klage einerseits und den Ansprüchen der konkret geschädigten Verbraucher andererseits her. Neben der Eintragung von Ansprüchen kommt dem Klageregister die zusätzliche Funktion zu, Musterfeststellungsklagen und -urteile bekannt zu machen, §§ 607, 609, 612 ZPO. Für die Eintragung in das Klageregister ist aus Sicht des Verbrauchers i. d. R. keine anwaltliche Vertretung vorgeschrieben.[202]

Wie in Kapitel 5.4.3.1 auf Seite 154 dargestellten Zivilprozess beginnt auch die Musterfeststellungsklage mit der Erhebung der Klage. Grundvoraussetzung ist hierbei, dass von den Feststellungszielen der Klage mindestens die Ansprüche von zehn Verbrauchern abhängen. Darüber hinaus müssen mindestens fünfzig Verbraucher zwei Monate nach der öffentlichen Bekanntmachung der Klage wirksam ihre Ansprüche im Klageregister angemeldet haben.[203] Während der Rechtshängigkeit der Klage kann kein weiterer Verbraucher gegen den Dienstanbieter Klage erheben, sofern er sich mit dieser Klage auf denselben Lebenssachverhalt berufen möchte, § 610 ZPO.

Ein im Rahmen der Musterfeststellungsklage ergangenes Urteil wird im Klageregister öffentlich bekannt gemacht. Gegen das Urteil kann regelmäßig das Rechtsmittel der Revision vor dem Bundesgerichtshof eingelegt werden, §§ 543 i. V. m. 614 ZPO. Für die Revision gelten die allgemeinen Bestimmungen der Zivilprozessordnung. Auch die (endgültige) Rechtskraft eines Urteils ist im Klageregister bekannt zu machen. Die Rechtskraft „bindet das zur Entscheidung eines Rechtsstreits zwischen einem angemeldeten Verbraucher und dem Beklagten berufene Gericht, soweit dessen Entscheidung die Feststellungsziele und den Lebenssachverhalt der Musterfeststellungsklage betrifft.“[204] Die Durchsetzung der individuellen Ansprüche der Verbraucher bleibt – trotz Musterfeststellungsklage – regelmäßig Individualprozessen vorbehalten, d. h. im Rahmen der Musterfeststellungsklage würde z. B. festgestellt, *ob* eine Dienstanbieter rechtswidrig gehandelt hat und *ob* dadurch ein Schaden entstanden ist. In den daran anschließenden Einzelverfahrenen der Verbraucher wird sodann geklärt, *wie hoch* der Schaden des Einzelnen ist. Eine Ausnahme von der Notwendigkeit, seine Ansprüche im Anschluss an die Musterfeststellungsklage im Einzelverfahren durchzusetzen, besteht insbesondere, wenn ein Musterfeststellungsverfahren mit einem Vergleich endet.

§ 611 ZPO sieht vor, dass ein gerichtlicher Vergleich mit Wirkung für und gegen die angemeldeten Verbraucher geschlossen werden kann. Ein Vergleich hat Regelungen über die auf die angemeldeten Verbraucher entfallenden Leistungen, den von den angemeldeten Verbrauchern zu erbringenden

[201] Pressemittelung des BMJV unter: https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2018/061418_MFK.html.

[202] Gleichwohl wird teilweise kritisiert, dass die Anforderungen an eine wirksame Eintragung für Verbraucher ohne das Hinzuziehen eines Rechtsanwalts nur schwer möglich ist, vgl. https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/musterfeststellungsklage-soll-bis-1112018-kommen_210_450624.html und *Halfmeier*, ZRP 2017, S. 201 (203), der die Vorstellung, die Verbraucher könnten die Eintragung ohne Hilfe eines Rechtsanwalts vornehmen, sogar als abwegig bezeichnet. Er sieht die „anwaltliche Betreuung einer entsprechenden Anspruchsbündelung“ als sinnvoll an und empfiehlt zusätzlich eine enge Abstimmung mit der klagenden Einrichtung, um die Musterfeststellungsklage und die Einzelverfahren bestmöglich aufeinander abstimmen zu können.

[203] *Waclawik*, NJW 2018, S. 2921 (2923). Nach § 204 I BGB wird im Rahmen der Musterfeststellungsklage die Verjährung für einen Anspruch gehemmt, den ein Gläubiger zu dem zu der Klage geführten Klageregister wirksam angemeldet hat, wenn dem angemeldeten Anspruch derselbe Lebenssachverhalt zugrunde liegt wie den Feststellungszielen der Musterfeststellungsklage.

[204] *Waclawik*, NJW 2018, S. 2921 (2923).

Nachweis der Leistungsberechtigung, die Fälligkeit der Leistungen und die Aufteilung der Kosten zwischen den Parteien zu enthalten. Ein Vergleich setzt die Genehmigung des Gerichts voraus, das den Vergleich regelmäßig dann zu genehmigen hat, wenn es ihn unter Berücksichtigung des bisherigen Sach- und Streitstandes als angemessene gütliche Beilegung des Streits erachtet. Da ein Vergleich regelmäßig unanfechtbar ist, werden die angemeldeten Verbraucher über den Vergleich in Kenntnis gesetzt. Für sie besteht sodann die Möglichkeit zum Austritt innerhalb einer festgelegten Frist, der regelmäßig schriftlich bei Gericht erklärt werden muss, sofern ein Verbraucher von der Möglichkeit des Austritts Gebrauch machen möchte. Sofern weniger als 30 % der angemeldeten Verbraucher von der Möglichkeit des Austritts Gebrauch gemacht haben, wird der Vergleich für diejenigen Verbraucher wirksam, die nicht ihren Austritt erklärt haben. Die Möglichkeit des Vergleichs bildet insbesondere deswegen ein „Herzstück“ der Musterfeststellungsklage, da es – sowohl aus Sicht der Gerichte als auch aus Sicht der Verbraucher – wenig sinnvoll und effizient ist, den Einzelanspruch jedes Verbrauchers individuell zu prüfen.[205]

Das Kostenrisiko der Musterfeststellungsklage trägt regelmäßig die klagebefugte Einrichtung – also i. d. R. der klagende Verbraucherschutzverband. Um das finanzielle Risiko des Verbraucherschutzverbandes tragbar zu machen, sieht die Musterfeststellungsklage eine (fiktive) Wertobergrenze von 250.000 Euro vor.[206] Somit liegt in der Musterfeststellungsklage eine erhebliche Verbesserung für die Verbraucher begründet, die für die Feststellung von (ggf. im Einzelfall geringfügigen) Ansprüchen zunächst lediglich ihren Anspruch anmelden müssen, jedoch weder dem Nervenkrieg vor Gericht, noch dem finanziellen Risiko des Rechtsstreits ausgesetzt werden. Ein Nachteil besteht darin, dass Verbraucher auf die Unterstützung/Initiative einer klagebefugten Einrichtung angewiesen sind.

5.5 Stärkung der Verbraucher

Das nachfolgende Unterkapitel thematisiert zunächst mögliche Benachteiligungen von Verbrauchern in Bezug auf das digitale Erbe bei der Dienstnutzung. Sodann soll das Unterkapitel untersuchen, welche Möglichkeiten bestehen, die Situation der Verbraucher zu verbessern, um insgesamt eine Stärkung der Verbraucher in Bezug auf ihren digitalen Nachlass zu erreichen.

5.5.1 Mögliche Benachteiligungen von Verbrauchern

Vergleicht man die in diesem Kapitel untersuchten AGB mit den von den sechs ausgewählten Dienstanbietern angebotenen Diensten, so fallen insbesondere drei Dinge auf:

1. In einigen Diensten wird in den AGB zwar deutlich erklärt, dass der Dienstnutzer einen digitalen Wert – wie beispielsweise eine digitale Buchdatei – nicht kauft, sondern lediglich eine Lizenz erwirbt, trotzdem wird im Rahmen der Dienstnutzung zum Teil auch der Begriff „Kaufen“ benutzt.

[205] *Halfmeier*, ZRP 2017, S. 201 (204).
[206] Hierzu durchaus kritisch *Halfmeier*, ZRP 2017, S. 201 (204).

2. Die meisten Dienstanbieter sind (noch) nicht darauf vorbereitet, dem Dienstnutzer direkt im Dienst rechtskonforme Möglichkeiten zu ermöglichen, seinen digitalen Nachlass vorzubereiten.

3. Die wenigen dem Dienstnutzer bereits heute zur Verfügung stehenden Mittel, im Rahmen der Dienstnutzung Vorkehrungen für seinen digitalen Nachlass zu treffen, könnten insofern missverständlich sein, als sie lediglich über den vom Dienstanbieter angebotenen Umfang, den digitalen Nachlass vorzubereiten, nicht aber über die gesetzlichen Rahmenbedingungen informieren.

5.5.1.1 Benutzung des Begriffs „Kaufen“

Auch wenn Dienstnutzer für digitale Werte wie z. B. Filmdateien i. d. R. nur eine Lizenz zur privaten Nutzung erhalten und somit nicht Eigentümer des digitalen Wertes werden, und Dienstanbieter in ihren AGB auf diesen Umstand auch grundsätzlich hinweisen, so verwenden die Dienstanbieter (mindestens) im Dienst selbst häufig trotzdem den Begriff des „Kaufens“.

Insbesondere verwenden Anbieter einen „Kaufen“ oder „Jetzt Kaufen“-Button. Sofern der Dienstnutzer in seinem Account angemeldet ist, wird der zahlungspflichtige Vorgang durch das Drücken des Buttons häufig ohne weitere bestätigende Handlung des Dienstnutzers durchgeführt. Einige Anbieter verwenden demgegenüber auch einen Button, der zunächst lediglich mit einem Betrag – z. B. 1,99 Euro – gekennzeichnet ist. Nach dem Drücken des Buttons wird der Dienstnutzer aber auch in diesem Fall darüber in Kenntnis gesetzt, dass der Artikel nun „gekauft“ wurde und heruntergeladen werden kann.

Wie bereits in Kapitel 5.4.2.1 auf Seite 149 festgestellt wurde, ist eine *zeitliche Beschränkung des Nutzungsrechts* durch die AGB des Dienstanbieters regelmäßig nur dann wirksam, wenn beim Nutzer der Eindruck erweckt wird, dass er die Inhalte käuflich erwirbt, etwa durch einen Button, „Jetzt Kaufen“, den er anklicken muss.[207]

Den Dienstanbietern kann zwar unterstellt werden, dass die Benutzung des Wortes „Kaufen“ grundsätzlich zum Schutz der Verbraucher erfolgt, damit diese nicht in Unwissenheit eine kostenpflichtige Aktion durchführen. Doch scheint die Benutzung des Begriffs „Kaufen“ im Zusammenhang mit dem kostenpflichtigen Erwerb einer zeitlich beschränkten Lizenz unpassend und somit für die Verbraucher benachteiligend zu sein.

5.5.1.2 Fehlende Unterstützung in der Vorbereitung eines digitalen Nachlasses

Nur wenige Dienstanbieter bieten ihren Dienstnutzern bisher überhaupt eine Unterstützung, wenn diese Vorkehrungen für ihren digitalen Nachlass treffen möchten. Insbesondere bieten sie nicht die Möglichkeit, z. B. die Kontaktinformationen des/r Erben sowie die Wünsche des Dienstnutzers rund um das Vererben der im Dienst ggf. entstandenen digitalen Werte in seinem Nutzeraccount zu hinterlegen und ggf. Erben über das Bestehen des Nutzeraccounts zu informieren.

[207] *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 24 f.

Dass Dienstanbieter ihre Dienstnutzer bisher in diesen Angelegenheiten nicht unterstützen, mag mindestens auch mit daran liegen, dass den meisten Dienstnutzern nicht bewusst ist, dass im Rahmen der Nutzung eines Online-Dienstes ggf. ideelle und/oder materielle, vererbbare Werte entstehen können. Entsprechend niedrig wird derzeit die Nachfrage der Dienstnutzer an Unterstützung durch die Dienstanbieter ausfallen. Aus Sicht der Dienstanbieter ist jedoch zumindest auch zu unterstellen, dass es für die Dienstanbieter regelmäßig profitabler sein dürfte, ihre Dienstnutzer nicht dabei zu unterstützen, ihren digitalen Nachlass vorzubereiten. So wird der Dienstanbieter regelmäßig beispielsweise von vor dem Tod des Erblassers nicht abgerufenem Guthaben profitieren, wenn der Dienstnutzer keine Vorkehrungen für seinen digitalen Nachlass getroffen hat, Erben ggf. von der Nutzung des Dienstes durch den Erblasser keine Kenntnis hatten und sich daher auch nicht an den Dienstanbieter wenden. Dabei wäre es Dienstanbietern ohne großen Aufwand möglich, entsprechende Funktionalitäten im Dienst zu ergänzen, die sich u. a. darauf beziehen könnten,

- dem Dienstnutzer die Möglichkeit zu bieten, den Kontakt zu seinem/n Erben in Nutzeraccount zu hinterlegen,
- dem Dienstnutzer eine Wahlmöglichkeit zu bieten, wie im Falle seines Todes mit den im Nutzeraccount entstandenen digitalen Werten verfahren werden soll (z. B. Löschen aller Accountdaten oder Herausgabe an die Erben bei einem Social-Media-Account)
- im Todesfall des Dienstnutzers dessen Erben über die Existenz des Nutzeraccounts zu informieren.[208]

5.5.1.3 Missverständliche Unterstützung in der Vorbereitung eines digitalen Nachlasses

Die wenigen Möglichkeiten, die einige Dienstanbieter ihren Nutzern bereits heute zur Verfügung stellen, um Vorkehrungen für ihren digitalen Nachlass zu treffen, könnten insofern missverständlich sein, als sie lediglich über den vom Dienstanbieter angebotenen Umfang, den digitalen Nachlass vorzubereiten informieren, den Dienstnutzer aber nicht (zusätzlich) darüber informieren, was aus rechtlicher Sicht mit seinem Nutzeraccount – bzw. mit den im Rahmen des Nutzeraccounts entstandenen digitalen Werten – nach seinem Ableben geschehen wird, wenn er keine Vorkehrungen für seinen digitalen Nachlass trifft.

Ein Beispiel hierfür ist die von Facebook vorgesehene Möglichkeit, einen Nachlasskontakt anzugeben. Diesbezüglich erklärt Facebook seinen Nutzern:

[208] Auch wenn der Dienstanbieter i. d. R. höchstens über die Erben verbindliche Kenntnis über den Todesfall des Dienstnutzers erhalten dürfte, so könnten trotzdem Mechanismen vorgesehen werden, die den/die im Dienst hinterlegten Erben über die Existenz des Accounts informieren, wenn sich ein Dienstnutzer über einen längeren Zeitraum nicht im Dienst zurückgemeldet hat. Hierfür könnte der Dienstnutzer ggf. sogar selbst den Zeitraum bestimmen und auch auswählen, wie oft er vom Dienstanbieter „gemahnt“ werden möchte, bevor die Meldung an die/den Erben erfolgt. In Verbindung mit seiner Wahlmöglichkeit – insbesondere in Bezug auf ideelle Werte wie Social-Media-Beiträge – könnte der Nutzeraccount nach den verstrichenen „Mahnungen“ auch gelöscht werden, sofern der Dienstnutzer nicht den Zugriff durch seine Erben wünscht.

„Ein Nachlasskontakt ist eine Person, die du auswählst, damit sie sich um dein Konto kümmert, wenn es in den Gedenkzustand versetzt wird [...]. Dein Nachlasskontakt kann Folgendes tun: [...]

- Beiträge selbst dann ansehen, wenn du deine Privatsphäre-Einstellungen auf **nur ich** festgelegt hattest. [...]
- Gedenkbeiträge löschen.
- Ändern, wer Beiträge sehen kann, in denen du markiert wurdest. [...]
- Neue Freundschaftsanfragen beantworten [...].
- Das Entfernen deines Kontos anfordern. [...]
- Du kannst es deinem Nachlasskontakt gestatten, eine Kopie deiner auf Facebook geteilten Inhalte herunterzuladen.

[...] Folgendes kann dein Nachlasskontakt nicht tun:

- Sich bei deinem Konto anmelden.
- Deine Nachrichten lesen.
- Deine Freunde entfernen oder neue Freundschaftsanfragen versenden. [...]“[209]

Auf der Seite werden weiterführende Informationen zum Facebook-Nachlasskontakt sowie der Menüpunkt zu den Nachlass-Einstellungen verlinkt. In seinen „Nachlass“-Einstellungen kann der Nutzer dem Nachlasskontakt erlauben, von dem Konto im Gedenkzustand ein Archiv der geteilten Informationen herunterzuladen. Zugriff auf Informationen wie z. B. Nachrichten oder Fotos, die der Nutzer automatisch synchronisiert, aber nicht gepostet hat, gewährt Facebook nur „möglicherweise“ und nur „wenn ein gültiges Testament oder eine andere wirksame Einwilligung mit einem eindeutigen Einverständnis vorliegt“.[210]

Problematisch könnte sein, dass sich die Facebook-Nutzer auf Basis der von Facebook bereitgestellten Informationen ggf. „in Sicherheit“ wähnen, wenn sie keinen Nachlasskontakt angeben, sofern sie wünschen, dass nach ihrem Tod niemand Zugriff auf ihre Daten erhalten soll. Sprich: Die Möglichkeit, einen Nachlasskontakt anzugeben und die hierzu an den Dienstnutzer gerichteten o. g. Informationen könnten beim Dienstnutzer den Eindruck erwecken, dass seinerseits keine Aktion erforderlich ist, sofern er gerade nicht wünscht, dass in seinem Todesfall jemand Zugriff auf seine Daten erhält. Auch könnte ggf. beim Dienstnutzer der Eindruck entstehen, er könne durch die Angabe eines Nachlasskontakts Zugriffe der (anderen) Erben ausschließen.

[209] Facebook Hilfebereich, https://www.facebook.com/help/1506822589577997?ref=tos.
[210] Facebook-Hilfebereich, https://de-de.facebook.com/help/408044339354739.

5.5.2 Empfehlungen zur Stärkung des Verbrauchers

Insbesondere ist in den nachfolgenden Abschnitten zu diskutieren, inwiefern die Notwendigkeit von Gesetzesänderungen und -ergänzungen besteht, welche Empfehlungen an Dienstanbieter gegeben werden können, um die Situation der Verbraucher zu verbessern, und inwiefern Verbraucher selbst Einfluss auf eine Verbesserung in Bezug auf ihren digitalen Nachlass nehmen können.

5.5.2.1 Gesetzesänderungen und -ergänzungen

Die Darstellung der AGB wichtiger Anbieter in Bezug auf deren Regelungsinhalte zum digitalen Nachlass im Vergleich zu der Dienstnutzung sowie die Bewertung der AGB ergaben zwar zumindest potenzielle Benachteiligungen der Verbraucher, diese bedürfen aus Sicht der Autoren der vorliegenden Studie jedoch keine Änderungen und/oder Ergänzungen des AGB-Rechts. Die Schutzvorkehrungen der §§ 305 ff. BGB sind insofern vollständig, als Verbraucher vollumfassend vor benachteiligenden AGB-Klauseln geschützt werden. Vielmehr regen die Autoren die Weiterführung der Diskussion um die Rechtsdurchsetzung von Ansprüchen der Verbraucher als zentrales Element an, damit sich in Zukunft Klageformen etablieren können, die Verbraucher in die Lage versetzen, sich effektiv gegen potenzielle Benachteiligungen zu Wehr setzen zu können, ohne u. a. vor jahrelangen Gerichtsverfahren und dem damit einhergehenden finanziellen Risiko zurückschrecken zu müssen.

Kritiker begrüßen zwar nachdrücklich das Bestreben, die Verbraucher zu stärken, jedoch bewerten sie die neue Musterfeststellungsklage als unzureichendes bzw. ungeeignetes Mittel, eine Stärkung der Verbraucher zu bewirken.[211]

Einen grundsätzlichen Kritikpunkt bildet zunächst der Umstand, dass Verbraucherverbände lediglich die grundsätzlichen Fragen (z. B. Rechtswidrigkeit und Schaden im Allgemeinen) gerichtlich klären lassen können, Verbraucher im Nachgang an die Feststellungsklage die Höhe ihres individuellen Schadens sowie dessen Durchsetzung trotzdem selbst vor Gericht einklagen müssen. Auch sehen Kritiker in dem Umstand, dass die Verbraucher im Rahmen der Musterfeststellungsklage nicht selbst klagen dürfen, ein „klares Misstrauensvotum [...] gegen die Verbraucher“, da ihnen nicht zugetraut würde, eigenverantwortlich darüber entscheiden zu können, ein Kollektivverfahren einzuleiten.[212] In diesem Zusammenhang wird auch kritisiert, dass die klagebefugten Verbraucherverbände häufig nicht über ausreichende (personelle und finanzielle) Ressourcen verfügen, zusätzlich zu ihren bisherigen Aufgaben langwierige und komplexe Verfahren für die Verbraucher zu führen – selbst wenn es potenziell viele Geschädigte gäbe, ist die Chance, dass Verbraucherschutzverbände eine Musterfeststellungsklage als Mittel zur Unterstützung der Verbraucher nutzen, daher im Auge vieler Kritiker als gering einzustufen. Auch davon abgesehen wird die Beschränkung der Klagebefugnis als hinderlich für die Rechtsdurchsetzung eingestuft.

[211] So z. B. kritisch: Kornmeier, Geplante Musterfeststellungsklagen – eine juristische Luftnummer?, unter: https://www.tagesschau.de/inland/justiz-musterfeststellungsklagen-101.html; *Halfmeier*, ZRP 2017, S. 201 (202); *Stadler*, VuR 2018, S. 87 (87).

[212] *Halfmeier*, ZRP 2017, S. 201 (202).

Diesen Kritikpunkten stehen die nicht abstreitbaren Vorteile der Musterfeststellungsklage gegenüber. Im Vergleich zu Alternativen, wie z. B. die vielfach geforderte Sammelklage, dauert das Verfahren deutlich kürzer, da gerade nicht die einzelnen Schäden geprüft und festgestellt werden müssten. Darüber hinaus trägt der Verbraucher kein (bzw. kaum ein) finanzielles Risiko des Verfahrens und hat mit dem Verfahren auch „erst einmal nichts zu tun, sondern könne abwarten, ob die spätere eigene Klage Erfolg haben könnte."[213] In diesem Sinne werden durch das Instrument der Musterfeststellungsklage regelmäßig die wichtigsten Gründe, die Verbraucher von der Durchsetzung ihrer Rechte abhält, adressiert.

Insbesondere die Nachteile in Bezug auf die Notwendigkeit, die individuellen Ansprüche im Anschluss an die Musterfeststellungsklage selbst durchzusetzen – sofern diese nicht mit einem Vergleich endet – sollten jedoch in Zukunft weiterverfolgt und -diskutiert werden. In diesem Zusammenhang ist insbesondere der Entwurf der *Richtlinie des Europäischen Parlaments und des Rates über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher* im Auge zu behalten.

Als Gegenvorschlag zur deutschen Musterfeststellungsklage wurde unterdessen u. a. unterbreitet, für Fälle mit hohen Schadensersatzsummen „einige wenige geeignete Verfahren als Musterprozesse [zu führen] – beschleunigt, konzentriert und gut strukturiert. Alle anderen Klagen sollten währenddessen ausgesetzt werden. Sobald der Bundesgerichtshof über die Musterprozesse entschieden habe, könnten auf Basis dieses Urteils die anderen Verfahren zu einem Abschluss gebracht werden."[214] Um dieses Ziel zu erreichen, wären laut Einschätzung der Kritiker lediglich geringfügige Ergänzungen der Zivilprozessordnung erforderlich. Für geringfügige Schäden von Verbrauchern, für die im Einzelfall eine Klage zu aufwendig wäre, könne laut Kritikern an der Musterfeststellungsklage festgehalten werden, jedoch mit der Ergänzung, dass die Verbraucherschutzverbände ein Urteil erreichen können, mit dem der Dienstanbieter zur Zahlung eines Schadenersatzes verurteilt werden könne.

Eine weitere Alternative zur deutschen Musterfeststellungsklage wurde insbesondere auch im Zusammenhang mit dem AGB-Recht diskutiert: Die gerichtliche Anordnung der Folgenbeseitigung nach erfolgreicher Unterlassungs- oder Feststellungsklage.[215] Hintergrund des Vorschlags ist, dass sich im Anwendungsbereich von Unterlassungs- und Musterfeststellungsklagen auch eine Vielzahl von Fällen findet, in denen es dem Verbraucher nicht um Schadensersatz, sondern z. B. um die Rückerstattung von (zu Unrecht) erhobener Gebühren und sonstiger Entgelte geht, bei denen sich der Dienstanbieter auf unwirksame AGB-Klauseln stützt. In diesen Fällen steht zwischen den Dienstanbietern und Verbrauchern eine direkte Vertragsbeziehung, der Dienstanbieter kann also regelmäßig selbst feststellen, an wen er welchen Betrag zurückerstatten muss. Somit könnte für den Verbraucher im Vergleich zur bloßen Musterfeststellungsklage vorteilhaft sein, wenn eine gerichtliche Anordnung – z. B. auf Basis eines Antrags eines klageberechtigten Verbandes – die Unterlassung und/oder die Anordnung zur Rückerstattung von Gebühren/sonstigen Entgelten an die Verbraucher beinhalten würde. In diesem Fall bestünde für die Verbraucher der nicht zu unterschätzende Vorteil, ihre (individuellen)

[213] Siehe https://www.deutschlandfunk.de/verbraucherschutz-barley-musterfeststellungsklage-besser.694.de.html?dram:article_id=432026.

[214] Kornmeier, Geplante Musterfeststellungsklagen – eine juristische Luftnummer?, unter: https://www.tagesschau.de/inland/justiz-musterfeststellungsklagen-101.html.

[215] *Stadler*, VuR 2018, S. 87 (87).

Ansprüche nicht noch im Nachgang an eine Musterfeststellungsklage durchsetzen zu müssen. Sie erhielten vielmehr ohne weitere notwendige Schritte einen Vollstreckungstitel. Insbesondere für Branchen, in denen es kein allgemein akzeptiertes Ombudsmannverfahren gibt – mit diesen ließ sich eine ähnliche Wirkungen bereits in der Vergangenheit ermöglichen – und/oder in denen es gerade nicht um individuelle Schadensberechnungen geht, scheint dieser Vorschlag ein sinnvoller und wünschenswerter Weg zu sein.[216]

Grundlegende Voraussetzung für die Entscheidung über die Nutzung eines Dienstes einerseits sowie für eine effektive Rechtsdurchsetzung andererseits ist, dass die Verbraucher sich für die Nutzung eines Dienstes in Bezug auf ihren digitalen Nachlass *informiert* entscheiden können, d. h. vom Dienstanbieter bereits vor/zu Beginn der Dienstnutzung umfassend über die wichtigsten Aspekte des digitalen Nachlasses informiert werden. In diesem Zusammenhang wird für weitere Ausführungen insbesondere auf Kapitel 4.2.2 auf Seite 106 verwiesen, das dem Gesetzgeber empfiehlt, die Öffnungsklausel des EG 27 S. 2 DSGVO zu nutzen, um die datenschutzrechtlichen Informationspflichten von Dienstanbietern auf den postmortalen Datenschutz zu erweitern, und Kapitel 5.5.2.2, das sich mit seiner Empfehlung, diese Informationspflichten auf alle wichtigen Aspekte des digitalen Nachlasses zu erweitern und ggf. die Transparenz durch einen Informationssteckbrief zum digitalen Nachlass weiter zu fördern, direkt an die Dienstanbieter richtet, verwiesen.

Bei den in diesem Abschnitt genannten Empfehlungen bleibt zu berücksichtigen, dass diese ggf. nur gegenüber nationalen Dienstanbietern, allenfalls auf europäischer Ebene, durchgesetzt werden können.

5.5.2.2 Informationspflichten der Dienstanbieter

Den Dienstanbietern kann zunächst empfohlen werden, ihre Dienstnutzer in angemessener Form über deren Rechte in Bezug auf das digitale Erbe aufzuklären. Hierbei soll es sich ausdrücklich nicht um weitreichende und detaillierte Informationen zum gesamten Erb- und postmortalen Datenschutzrecht handeln, sondern um eine kurze Information, die auf die wichtigsten (potenziellen) Fragen der Dienstnutzer bei der Nutzung des konkreten Dienstes eingehen, wie z. B.

1. „Sind die von mir gekauften digitalen Bücher, Musik- und Filmdateien vererbbar?“
2. „Kann ich von mir gekaufte virtuelle Spielwährung und -Gegenstände sowie von mir erspielte Spielstände vererben?“
3. „Kann ich verbieten oder anordnen, dass meine Erben nach meinem Tod auf meine personenbezogenen Daten Zugriff erhalten?“

Wie bereits in Kapitel 4.2.2 auf Seite 106 dargestellt wurde, handelt es sich bei solchen Hinweisen von Dienstanbietern nicht nur um Hinweise auf die zivil- bzw. erbrechtliche Rechtslage, sondern ggf. auch um Hinweise zum postmortalen Datenschutz, die der Erblasser regelmäßig benötigt, um informierte Entscheidungen über den Zugriff auf seine Daten nach seinem Tod treffen zu können. Kapitel 4.2.2

[216] *Stadler*, VuR 2018, S. 87 (88).

auf Seite 106 diskutierte für das Datenschutzrecht die Notwendigkeit, die Informationspflichten der Dienstanbieter hinsichtlich einer „Datenverarbeitung post mortem“ auszuweiten und hierfür die Öffnungsklausel des EG 27 S. 2 DSGVO zu nutzen.[217] Wünschenswert wäre es, dass Dienstanbieter hierbei nicht nur die datenschutzrechtliche Sicht (Frage 3), sondern auch die erbrechtliche Sicht (Fragen 1 und 2) berücksichtigen und diese ihren Dienstnutzern zusätzlich transparent machen.

Um die Informationspflichten im Datenschutzrecht angemessen, verständlich und auch schnell erfassbar zu machen, wurde in den letzten Jahren der Einsatz von Bildsymbolen beim Erbringen der datenschutzrechtlichen Informationspflichten diskutiert.[218] Die Entwicklung geeigneter Bildsymbole, die zum einen alleinstehend verständlich und zum anderen frei von Fehlinterpretationspotenzial sind, erweist sich jedoch bisher als schwierige Herausforderung, weshalb weitere Alternativen wie z. B. der sogenannte Datenschutz-Steckbrief, eine Kombination aus visuellen Elementen und kurzen Informationstexten, der die i. d. R. sehr langen Datenschutzerklärungen als eine Art „Kompaktinformation“ ergänzen könnte, diskutiert werden.[219]

Die Orientierung an dem Vorschlag eines Datenschutz-Steckbriefs könnte zu einem (freiwilligen) Steckbrief zum digitalen Nachlass führen, im Rahmen dessen Dienstanbieter ihren Dienstnutzern mit grafischen Symbolen und kurzen Informationstexten die wichtigsten Informationen zu den Aspekten des digitalen Nachlasses zusammenfassen. Der Einsatz eines solchen Informations-Steckbriefs würde nicht nur einen großen Vorteil für die Dienstnutzer in Bezug auf mehr Transparenz im digitalen Nachlass mit sich bringen, sondern könnte potenziell auch ein Wettbewerbsvorteil für die Dienstanbieter sein: Klären diese transparent über die für ihren Dienst relevanten Aspekte des digitalen Nachlasses auf (und zeigen ggf. auch Möglichkeiten auf, direkt im Dienst eine Wahl bzgl. des digitalen Nachlasses zu treffen, vgl. nachfolgenden Unterabschnitt), so könnten sich Dienstnutzer bewusst für diesen Dienstanbieter entscheiden.

Sofern ein wie hier vorgeschlagener Steckbrief zum digitalen Nachlass nicht von den Dienstanbietern selbst aufgegriffen würde, kann alternativ auch unabhängigen Stellen wie z. B. der Stiftung Warentest oder Verbraucherschutzverbänden empfohlen werden, die Qualität verschiedener Dienstanbieter in Bezug auf den digitalen Nachlass zu bewerten und die Informationen allgemeinverständlich und im Kurzüberblick – z. B. durch den vorgeschlagenen Steckbrief zum digitalen Nachlass – aufzuarbeiten.

Möglich wäre es auch, zukünftig gar über ein Siegel zum digitalen Nachlass nachzudenken, mit dem Dienstanbieter für einen besonders verbraucherfreundlichen Umgang mit dem digitalen Nachlass werben können. Primär sollte jedoch (direkt) durch die Dienstanbieter versucht werden, zugunsten der Verbraucher für mehr Information und Auswahlmöglichkeiten zu sorgen („Pflicht“). Ein Vergleich durch unabhängige Stellen und/oder ein Siegel stellen insofern nachgelagerte Optionen dar („Kür“).

[217] Auch die *Datenethikkommission* empfiehlt in ihrem Gutachten aus Oktober 2019, S. 111, von der Möglichkeit der Öffnungsklausel Gebrauch zu machen, um Regelungen für den postmortalen Datenschutz zu erlassen.
[218] *Hansen*, in: INFORMATIK 2009, S. 1703.
[219] *Hansen*, in: BvD, S. 46 ff.

Abbildung 5.1: Steckbrief zum digitalen Nachlass als Möglichkeit der Information an Erblasser

5.5.2.3 Verbesserung der Transparenz der Anbieter-AGB

Sofern die AGB von Dienstanbietern Regelungen zum/mit Relevanz für den digitalen Nachlass enthalten, so kann die Transparenz aus Sicht des Verbrauchers bereits durch eine entsprechende Überschrift verbessert werden. AGB-Klauseln, die den Ausschluss einer Guthabenübertragung an Dritte, den Ausschluss der Rückerstattung von erworbenem Guthaben und/oder die Gültigkeit des erworbenen Guthabens betreffen, sollten aufgrund ihrer besonderen Bedeutung für den Verbraucher grundsätzlich deutlich hervorgehoben werden. Jedenfalls erscheint ein Verstecken solcher Klauseln in den AGB intransparent. Auch sollten Formulierungen wie „[Rückerstattungen sind ausgeschlossen. Eine Ausnahme besteht,] wenn es gesetzlich erforderlich ist.“ mit konkreten Beispielen versehen werden, um dem Verbraucher aufzuzeigen, in welchen Fällen die gesetzliche Erfordernis besteht. Die Verbesserung der Transparenz zu AGB-Klauseln mit Bezug zum digitalen Nachlass ließe sich darüber hinaus durch die Klarstellung verbessern, dass/ob Erben, Vorsorgebevollmächtigte und Betreuer „Dritte“ im Sinne der relevanten Klauseln sein sollen.

Die Frage, ob Dienstanbietern zu empfehlen ist, (sowohl in den AGB als auch im Rahmen der Dienstnutzung selbst) eine Alternative zum Wort „Kaufen“ zu benutzen, wenn Dienstnutzer einen digitalen Gegenstand lediglich lizenzieren und dieser ggf. nicht weitervererbbar ist, kann nicht abschließend bewertet werden. Mit dem dem Wort „Kaufen“ soll dem Verbraucher regelmäßig signalisiert werden, dass das Klicken des „Kaufen“-Buttons eine Aktion auslöst, die für den Verbraucher kostenpflichtig ist. Die Bewertung, ob, in welcher Häufigkeit und mit welcher Vehemenz Verbraucher in dem ggf. vorliegenden Umstand, einen „gekauften“ digitalen Gegenstand nicht weitervererben zu können, eine Benachteiligung sehen oder von diesem Umstand überrascht wären, kann diese Studie nicht leisten. Es ist jedoch zu vermuten, dass dem Verbraucher die Unterscheidung zwischen „Kaufen“ und beispielsweise „lebenslange Lizenz erwerben“, „lebenslange Erlaubnis zur Nutzung erwerben“

oder einfach „gebührenpflichtig erwerben“ verständlich dargestellt werden kann und er in den Formulierungen erkennt, dass das Klicken auf den Button eine für ihn kostenpflichtige Aktion auslöst. Wünschenswert wäre es in diesem Zusammenhang ggf., repräsentative Umfragen von Verbrauchern durchzuführen.

5.5.2.4 Vermeidung jeglicher Koppelung der Erben an den Dienst

Dienstanbietern ist darüber hinaus zu empfehlen, jegliche Koppelung zu vermeiden, die die (einfache und effektive) Durchsetzung eines digitalen Nachlasses an die Bedingung knüpft, dass es sich bei dem Erben ebenfalls um einen Nutzer des Dienstes handeln muss. Auch Benachteiligungen von Erben, die keine Dienstnutzer sind im Vergleich zu Erben, die Dienstnutzer sind, sind zu vermeiden. Solche Regelungen benachteiligen regelmäßig sowohl den Erblasser als auch den/die Erben in unangemessener Weise.

Dementsprechend sollte auch für die Möglichkeit, einen Nachlasskontakt im Nutzeraccount des Erblassers zu hinterlegen, insbesondere vorgesehen werden, dass es sich hierbei auch um Personen handeln kann, die nicht selbst Nutzer des Dienstes sind. Um die in Kapitel 5.4.2.4 auf Seite 152 erwähnte Kritik zu berücksichtigen, sollten Dienstanbieter auch die Möglichkeit vorsehen, mehrere Personen als Nachlasskontakt benennen zu können. Auch sollten u. a. Gebühren, die sich nur an Erben als „Nicht-Dienstnutzer“ richten, vermieden werden.

5.5.2.5 Angemessene Vorbereitung einer Account-Deaktivierung

Den Dienstanbietern kann darüber hinaus geraten werden, die Deaktivierung eines Nutzeraccounts, mit der die Einschränkung und/oder der Verlust eines ideellen oder finanziellen Wertes des digitalen Nachlasses verbunden ist, dem Dienstnutzer – und somit in dessen Todesfall ggf. auch seinen Erben – rechtzeitig anzuzeigen und dem Dienstnutzer durch eine einmalige Aktion, wie z. B. das erneute Einloggen in seinen Nutzeraccount, die Möglichkeit zu geben, die Deaktivierung zu verhindern.[220]

Insbesondere im Hinblick darauf, dass die Erben ggf. noch keine Kenntnis von dem Nutzeraccount des Erblassers haben, sollte die Benachrichtigung über die bevorstehende Deaktivierung des Accounts nicht nur im Nutzeraccount selbst, sondern über einen zusätzlichen Kanal – insbesondere per E-Mail-Benachrichtigung – erfolgen. Auch im Hinblick auf die Erben sollte die erstmalige Information über die bevorstehende Deaktivierung nach Möglichkeit bereits ca. 3-4 Wochen vor der Deaktivierung erfolgen, mit (mindestens) einer weiteren Erinnerung kurz vor der bevorstehenden Deaktivierung. Hiermit wird verhindert, dass sich Nachteile für die Erben ergeben, wenn diese den E-Mail-Account des Erblassers nur in unregelmäßigen und/oder größeren Zeitabständen abrufen. Den Erben selbst ist in diesem Zusammenhang zu empfehlen, alle ihnen bekannten E-Mail-Postfächer des Erblassers für einen Zeitraum von ca. 3-5 Jahren weiter abzurufen, um über bevorstehende Deaktivierungen von

[220] In Verbindung mit einer nicht zu kurz bemessenen Inaktivitätszeit vor der Schließung des Accounts ist sodann die Deaktivierung/Schließung eines Accounts regelmäßig zulässig, siehe: *Herzog/Pruns*, in: Der digitale Nachlass, § 5 Rn. 14

ihnen bis dahin nicht bekannten Nutzeraccounts des Erblassers Kenntnis nehmen zu können, sofern dies im konkreten Anwendungskontext rechtlich zulässig ist.

Aus erbrechtlicher Sicht ist hierbei zu beachten, dass – sofern ein E-Mail-Account auf mehrere Erben übergeht – dieser E-Mail-Account in den gemeinschaftlichen Nachlass fällt. Dieser ist grundsätzlich darauf ausgerichtet, möglichst bald auseinandergesetzt zu werden. Jedoch ist es sinnvoll, vor allem E-Mail-Accounts des Erblassers nicht vorschnell zu löschen, da immer mehr Rechnungen etc. ausschließlich per E-Mail verschickt werden. Aus erbrechtlicher Sicht wäre es daher wünschenswert, wenn die Erben eine Einigung dahingehend erzielen könnten, dass einer der Erben den E-Mail-Account weiter verwaltet. Diesem Erben könnte sodann empfohlen werden, den bestehenden Mechanismus des „E-Mail-Nachsendeauftrags“ bzw. des dauerhaften „E-Mail-Weiterleitungsauftrags“ an die E-Mail-Adresse des verwaltenden Erben zu nutzen.

5.5.2.6 Einräumen einer Wahlmöglichkeit

Zuletzt kann insbesondere Anbietern sozialer Netzwerkplattformen empfohlen werden, den Verbrauchern über die AGB eine Wahlmöglichkeit in Bezug auf ihren digitalen Nachlass einzuräumen. Wie in Kapitel 4.2.2 auf Seite 106 beschrieben, regelt unter anderem Xing in den AGB die Wahlmöglichkeit zwischen der Einsichtnahme der Erben in die Profildaten des Erblassers einerseits und dem Löschen der Profildaten andererseits. Eine solche Wahlmöglichkeit ist zu begrüßen.[221] Zugunsten der Verbraucher sollten die entsprechenden AGB-Klauseln so formuliert sein, dass die von dem Erblasser getätigte Wahl für den Dienstanbieter rechtsverbindlich ist und die Umsetzung nicht nur im vertraglich festgelegten Ermessen des Dienstanbieters liegt.

Auch wäre es wünschenswert, wenn Dienstanbieter eine (technische) Möglichkeit schaffen würden, die Wahlmöglichkeit aus Sicht des Verbrauchers in einfacher Weise umzusetzen. Hierfür könnte es sich z. B. anbieten, eine ähnliche Funktionsweise zu implementieren, wie sie in den Datenschutzeinstellungen in Nutzerprofilen von Social-Media-Plattformen vorgesehen ist, um die Sichtbarkeit des eigenen Profils durch „Freunde“, „Freunde von Freunden“, „alle“ usw. nach den individuellen Wünschen des Profilinhabers zu gestalten. Im Ergebnis könnte der Dienstnutzer zu Lebzeiten in seinem Profil somit festlegen, dass sein Profil im Todesfall gelöscht oder aber den Erben zur Einsichtnahme zur Verfügung stehen soll. Ein weiterer Vorteil der (technischen) Unterstützung, eine Wahlmöglichkeit in einfacher Weise wahrnehmen zu können, sowie des im vorherigen Kapitel beschriebenen Informations-Steckbriefs wäre zudem, dass der Dienstnutzer nicht nur in den AGB – die häufig gar nicht oder nur oberflächlich gelesen werden – sondern auch über einen entsprechenden Menüpunkt in seinem Nutzerprofil auf seinen digitalen Nachlass hingewiesen würde und sich somit die Chance der Kenntnisnahme durch den Nutzer vergrößert.

Bei der technischen Umsetzung könnte ggf. auch einem in Kapitel 4.2.2 auf Seite 106 genannten Nachteil begegnet werden, nämlich der, dass die (bloße) Wahlmöglichkeit der Vererbung oder rück-

[221] Dies bezieht sich insbesondere auf den Fall, dass der Erblasser seine Daten nach seinem Tod pauschal gelöscht wissen oder pauschal an seine Erben ausgehändigt wissen will. Vgl. die in Kapitel 4.2.2 auf Seite 106 beschriebenen Vor- und Nachteile.

standlosen Löschung von Daten sehr pauschal ist. Es ist zu unterstellen, dass es für die Dienstanbieter kein unverhältnismäßig großer Aufwand wäre zu unterscheiden, dass der Erblasser beispielsweise die im Dienst eingestellten Fotos an einen Erben weitergeben möchte, seine geschriebenen Privatnachrichten aber komplett gelöscht werden sollen.

Wichtig ist, dass die (technische) Möglichkeit der Umsetzung einer Wahlmöglichkeit nicht für sich alleine steht. Die zusätzliche Zusicherung einer Wahlmöglichkeit in den AGB ist unumgänglich, um dem Erblasser Rechtssicherheit zu geben, dass die von ihm getroffene und an den Dienstanbieter übermittelte Auswahl für den Dienstanbieter verbindlich ist. Hingegen käme eine bloße (technische) Möglichkeit der Umsetzung einer Wahlmöglichkeit regelmäßig nur einer Möglichkeit zur unverbindlichen Äußerung eines Wunschs gleich.

5.5.2.7 Awareness-Maßnahmen für Verbraucher

Bislang ist davon auszugehen, dass sich in letztwilligen Verfügungen derzeit nur in seltenen Ausnahmefällen Anweisungen finden, die sich speziell zum digitalen Nachlass äußern. Häufig ist für Erben nicht einmal ersichtlich, in welchen Online-Plattformen der Erblasser aktiv war und wo sich ggf. finanzielle und/oder ideelle digitale Werte verstecken. Erblassern ist zu Lebzeiten wiederum häufig weder bewusst, was mit ihren persönlichen Daten und finanziellen digitalen Werten nach ihrem Tod passieren wird, noch ist ihnen bewusst, dass sie darauf aktiv Einfluss nehmen können.

Es steht daher außer Frage, dass es notwendig ist, Verbraucher umfangreich für das Thema des digitalen Nachlasses zu sensibilisieren. U.a. muss dafür sensibilisiert werden, dass

- auf das digitale Erbe zu Lebzeiten aktiv Einfluss genommen werden kann,
- Internet-Accounts häufig den Tod des Erblassers überdauern, sodass von der eben genannten Möglichkeit Gebrauch gemacht werden sollte und
- insbesondere das Auffinden ideeller und finanzieller digitaler Werte für Erben deutlich erschwert wird, wenn sie unter Verwendung eines Pseudonyms genutzt werden und der Erblasser den Erben keine diesbezüglichen Informationen hinterlässt.

So schreibt *Seidler* zutreffend: „Nur wenn Nutzer über die rechtliche Ausgangslage informiert sind, können sie entsprechende Vorsorgemaßnahmen ergreifen, sollte diese nicht ihrem Willen entsprechen.“[222] Dementsprechend sind Initiativen wie die Kampagne „Machts gut“,[223] die im Jahr 2014 von der Verbraucherzentrale im Auftrag des Bundesministeriums für Justiz und für Verbraucherschutz durchgeführt wurde, zu begrüßen und die Ergebnisse, zu denen u. a. auch eine Muster-Vollmacht zum digitalen Nachlass sowie eine Muster-Liste für Internetzugangsdaten zählen, nach Möglichkeit dauerhaft und kostenlos für die Verbraucher zur Verfügung zu halten. Einen Vorschlag einer Muster-Vollmacht enthält auch die vorliegende Studie im Kapitel 9.1 auf Seite 345. Sofern sich die Rechtslage und/oder technische Gegebenheiten in Bezug auf das digitale Erbe bzw. die Durchsetzbarkeit

[222] *Seidler*, Digitaler Nachlass, S. 160.

[223] https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/digitaler-nachlass-letzter-wille-zu-gespeicherten-daten-12002.

des digitalen Nachlasses verändern sollten, wäre ggf. eine neue Kampagne (bzw. die Aktualisierung der bereitgestellten Informationen) wünschenswert. Sofern solche Kampagnen jedoch voraussetzen, dass Internetnutzer (z. B. durch eine entsprechende Abfrage einer Online-Suchmaschine) aktiv nach Informationsmaterial suchen, sollte der oben beschriebene Umstand Berücksichtigung finden, dass sich derzeit nur sehr wenige Menschen mit dem digitalen Nachlass befassen. Daher gilt es für die Zukunft zu erörtern, ob Awarenesskampagnen, die unterschiedliche Kanäle (z. B. Informationsaufbereitung im Internet, Printanzeigen, Beiträge im Rundfunk, Bürgerveranstaltungen) bedienen, der reinen Aufbereitung von Informationen über das Internet vorzuziehen sind.

Darüber hinaus gilt es zu erörtern, ob Kompetenzen im Bereich des digitalen Nachlasses auch in Schulen vermittelt werden sollten. Die sogenannten „Digital Natives“, also Menschen, die mit digitalen Technologien wie Smartphones, sozialen Netzwerkplattformen etc. aufgewachsen sind, verfügen zwar regelmäßig über eine hohe Kompetenz in der Nutzung digitaler Technologien, doch gilt es die junge Internetgeneration auch vor den Gefahren digitaler Technologien zu bewahren, also u. a. vor der Beeinflussung durch gezielte Falschnachrichten und vor negativen Konsequenzen durch die Preisgabe persönlicher Informationen im Internet. Die Notwendigkeit der Vermittlung von Medienkompetenzen in Schulen wurde daher bereits viel diskutiert,[224] ein Umbruch ist längst in Gange. Die Vermittlung von Kompetenzen im Bereich des digitalen Nachlasses in Schulen – insbesondere in den höheren Jahrgangsstufen – könnte daher ein naheliegender nächster Schritt sein, den es zu diskutieren gilt. Hierbei ist zu beachten, dass ein aktives Eingreifen durch Vertrag und/oder Testament i. d. R. erst mit Volljährigkeit möglich ist. Dies sollte insofern berücksichtigt werden, als dass davon auszugehen ist, dass das Thema auf Desinteresse stoßen könnte, wenn ein konkretes Handeln der Schüler (noch lange) nicht möglich ist.

5.6 Zusammenfassung

Zu den digitalen Werten gehören u. a. E-Books, digitale Musikdateien und digitale personenbezogene Daten wie Fotos, geschriebene Beiträge und „Likes“. Die Grundlage der Nutzung solcher digitalen Werte bei einem bestimmten Anbieter bilden i. d. R. die sogenannten Allgemeinen Geschäftsbedingungen (AGB), also für eine Vielzahl von Verträgen vorformulierte Vertragsbestimmungen. AGB unterstützen den schnellen und unkomplizierten Vertragsschluss zwischen Anbieter und Verbraucher, da die beiden Vertragsparteien keinen individuellen Vertrag aushandeln müssen.

Der Verbraucher als Dienstnutzer kann i. d. R. keinen Einfluss auf die Inhalte der AGB nehmen. Selbst wenn er mit einer oder mehreren der AGB-Klauseln nicht einverstanden wäre, so hätte er lediglich die Wahl, den Dienst zu den in den AGB stehenden Bedingungen zu nutzen oder sich einen alternativen Dienst bzw. Dienstanbieter zu suchen. Der Dienstanbieter befindet sich gegenüber dem Dienstnutzer daher regelmäßig in einer sehr starken Position. Trotzdem ist der Dienstnutzer dem Dienstanbieter nicht schutzlos ausgeliefert, da sich die wirksame Einbeziehung und die Wirksamkeit der AGB-Klauseln selbst an den §§ 305 ff. BGB messen lassen müssen, die einen Ausgleich schaffen

[224] Siehe u. a. https://www.deutschlandfunk.de/unterricht-wie-medien-schule-machen-koennen.2907.de.html?dram:article_id=412497, https://merton-magazin.de/wahrheit-oder-luege-warum-medienkompetenz-fuer-schueler-so-wichtig-ist.

zwischen der starken Position der Dienstanbieter und dem Potenzial, diese starke Position gegenüber den Verbrauchern (als Dienstnutzer) auszunutzen.

Vor diesem Hintergrund stellte dieses Kapitel zunächst diejenigen AGB-Klauseln der für diese Studie beispielhaft ausgewählten Anbieter PayPal, Microsoft, Apple, Amazon, Sony und Facebook dar, die die Vererbbarkeit digitaler Werte regeln und/oder auf sonstige Weise für den digitalen Nachlass relevant sind.

Die Bewertung dieser Regelungen sowie ein sich an die Bewertung anschließender Vergleich der Regelungen zum digitalen Nachlass in den AGB zu den konkreten Diensten ergab großes Potenzial, die Verbraucher in Bezug auf ihren digitalen Nachlass zu stärken. Insbesondere wurde diskutiert, inwiefern die Notwendigkeit von Gesetzesänderungen und -ergänzungen besteht, welche Empfehlungen zur Verbesserung der Situation der Verbraucher an Dienstanbieter gegeben werden können und inwiefern Verbraucher selbst Einfluss auf eine Verbesserung in Bezug auf ihren digitalen Nachlass nehmen können. Aus der Untersuchung lassen sich zusammenfassend folgende Erkenntnisse und Empfehlungen ableiten:

- Der Schutzumfang, den die §§ 305 ff. BGB in Bezug auf die wirksame Einbeziehung und die Wirksamkeit von AGB für Verbraucher vorsehen, scheint vollständig. Vielmehr sollte die Diskussion um die Rechtsdurchsetzung von Ansprüchen der Verbraucher fortgesetzt werden.

- Ein genereller Ausschluss der Vererblichkeit eines *Nutzerkontos* in AGB wird in der Literatur überwiegend für unwirksam erachtet. Eine *Lizenz an digitalen Werten* – wie z. B. Musik- oder Filmdateien – kann demgegenüber i. d. R. in den AGB wirksam auf die Lebzeit des Erblassers beschränkt werden. Ggf. sollte aber über eine repräsentative Umfrage geklärt werden, ob seitens der Verbraucher im Rahmen der AGB und im Rahmen der Dienstnutzung die Notwendigkeit besteht, das Wort „Kaufen“ von dem „Erwerb einer lebenslangen Lizenz“ abzugrenzen, um dem Verbraucher aufzuzeigen, dass ein digitaler Wert ggf. nach dessen Tod nicht vererbbar ist.

- Den Dienstanbietern ist zu empfehlen, ihre Dienstnutzer in angemessener – d. h. kurzer und allgemeinverständlicher – Form über deren Rechte in Bezug auf das digitale Erbe aufzuklären. Ggf. können sich Dienstanbieter hierfür ein Beispiel am sogenannten „Datenschutz-Steckbriefs“ nehmen und einen „Steckbrief zum digitalen Nachlass“ entwickeln.

- Greifen die Dienstanbieter die Empfehlung eines „Steckbriefs zum digitalen Nachlass“ nicht auf, so könnten ggf. unabhängige Institutionen wie Verbraucherschutzverbände oder die Stiftung Warentest diese Aufgabe in Form eines Anbietervergleichs übernehmen. Auch könnte ein „Siegel zum digitalen Nachlass“ entwickelt werden.

- Mehr Transparenz in den AGB können Dienstanbieter u. a. dadurch erreichen, dass sie Regelungen zum digitalen Nachlass durch eine entsprechende Überschrift kennzeichnen und AGB-Klauseln, die den Ausschluss einer Guthabenübertragung an Dritte o. ä. betreffen, deutlich hervorgehoben werden. Auch sollte klargestellt werden, ob Erben, Vorsorgebevollmächtigte und Betreuer „Dritte“ im Sinne der relevanten Klauseln sein sollen.

- Dienstanbietern ist darüber hinaus zu empfehlen, jegliche Koppelung zu vermeiden, die die (einfache und effektive) Durchsetzung eines digitalen Nachlasses an die Bedingung knüpft, dass es sich bei dem Erben ebenfalls um einen Nutzer des Dienstes handeln muss. Auch sind sonstige Benachteiligungen von Erben, die keine Dienstnutzer sind, im Vergleich zu Erben, die Dienstnutzer sind, zu vermeiden.
- Eine bevorstehende Deaktivierung eines Nutzeraccounts sollte der Dienstanbieter dem Dienstnutzer – und somit in dessen Todesfall ggf. auch seinen Erben – rechtzeitig (per E-Mail) anzeigen. Auch im Hinblick auf die Erben sollte die erstmalige Information über die bevorstehende Deaktivierung nach Möglichkeit bereits ca. 21 Tage vor der Deaktivierung erfolgen.
- Im selben Zusammenhang ist den Erben zu empfehlen, alle ihnen bekannten E-Mail-Postfächer des Erblassers – sofern rechtlich zulässig – für einen Zeitraum von ca. 3–5 Jahren weiter abzurufen, um über bevorstehende Deaktivierungen von ihnen bis dahin nicht bekannten Nutzeraccounts des Erblassers Kenntnis nehmen zu können.
- Dienstanbietern – insbesondere Anbietern sozialer Netzwerkplattformen – kann empfohlen werden, den Verbrauchern über die AGB eine Wahlmöglichkeit in Bezug auf ihren digitalen Nachlass einzuräumen, sodass sie z. B. zu Lebzeiten wählen können, dass ihr Account in ihrem Todesfall gelöscht werden soll, ohne dass Erben (vorher) Zugriff auf diesen erhalten. Zugunsten der Verbraucher sollten die entsprechenden AGB-Klauseln so formuliert sein, dass die von dem Erblasser getätigte Wahl für den Dienstanbieter rechtsverbindlich ist und die Umsetzung nicht nur im vertraglich festgelegten Ermessen des Dienstanbieters liegt.
- Das Einräumen einer Wahlmöglichkeit zum digitalen Nachlass des Verbrauchers könnte zusätzlich technisch unterstützt werden, um den Verbraucher in die Lage zu versetzen, in seinem Nutzeraccount zu verfügen, ob im Todesfall alle Daten gelöscht werden sollen, oder beispielsweise die Erben Zugriff auf sämtliche Fotos, nicht aber auf sonstige Beiträge, erhalten sollen.
- Da Erblassern derzeit häufig weder bewusst ist, was mit ihren persönlichen Daten und ihren finanziellen digitalen Werten nach ihrem Tod passieren wird, noch ihnen bewusst ist, dass sie darauf aktiv Einfluss nehmen können, ist zudem zu empfehlen, Verbraucher z. B. im Rahmen von Awarenesskampagnen für das Thema des digitalen Nachlasses zu sensibilisieren.

Bei einigen der genannten Empfehlungen bleibt zu berücksichtigen, dass diese ggf. nur gegenüber nationalen Dienstanbietern, allenfalls auf europäischer Ebene, durchgesetzt werden können.

Das Wichtigste in Kürze

Allgemeine Geschäftsbedingungen (AGB) sind für eine Vielzahl von Verträgen vorformulierte Vertragsbestimmungen. Sie unterstützen den schnellen und unkomplizierten Vertragsschluss zwischen einen Anbieter eines (Online-)Dienstes und dem Nutzer des Dienstes. Aus der Prüfung der AGB verschiedener, für diese Studie beispielhaft ausgewählter Dienstanbieter ergaben sich Empfehlungen, die die Dienstnutzer in Bezug auf ihren digitalen Nachlass stärken können, zum Beispiel:

- Die Dienstnutzer sollten in den Möglichkeiten, ihre Rechte gegenüber den Dienstanbietern gerichtlich durchsetzen zu können, gestärkt werden. Zum Beispiel sollen (weitere) Möglichkeiten diskutiert werden, durch den Zusammenschluss mit weiteren Betroffenen das finanzielle Risiko einer Klage zu senken.

- Dienstanbieter sollten ihre Dienstnutzer besser über die für den jeweiligen Dienst relevanten Aspekte des digitalen Nachlasses informieren – in kurzer und allgemeinverständlicher Weise.

- Erben sollten in Bezug auf ihr Erbe vom Dienstanbieter nicht benachteiligt werden, wenn/weil sie selbst nicht den Dienst des Dienstanbieters nutzen.

- Soweit rechtlich zulässig, sollten Erben alle ihnen bekannten E-Mail-Postfächer des Erblassers 3–5 Jahre weiter abrufen, um unbekannte Onlineaktivitäten des Verstorbenen zu erkennen und ggf. ideelle und finanzielle Werte aufzuspüren.

6 Vorsorge durch den Nutzer

Dieses Kapitel untersucht

- die rechtlichen Vorsorgemöglichkeiten, die schon zu Lebzeiten wirken, wenn ein Nutzer seine Rechte und Pflichten nicht mehr selbst wahrnehmen kann;
- die Trans- oder postmortale Vollmacht als rechtliche Vorsorgemöglichkeit zur Verwaltung des digitalen Nachlasses im Todesfall durch eine dritte Person;
- die Gestaltungsmöglichkeiten für den Sterbefall durch eine letztwillige Verfügung (Testament);
- die technischen und organisatorischen Verfahren, mit denen die Zugangsdaten zum digitalen Nachlass und entsprechende Nachweise für die Erben bereitgestellt werden können;
- die Möglichkeiten, wie die Erben und Bevollmächtigten ihre Berechtigung nachweisen können;
- die rechtlichen Gründe, warum Berechtigte ihre Identität nachweisen müssen;
- die technischen und organisatorischen Verfahren, mit denen Berechtigte ihre Identität nachweisen können.

6.1 Motivation

Trotz der rechtlichen Bewertung, die eine Vererbbarkeit und die Befugnisse von Stellvertretern bestätigt, ist eine private Vorsorge durch die Nutzer immer noch zu empfehlen, da die uneinheitliche Praxis der Dienstanbieter zu Rechtsunsicherheiten führt. Zudem erleichtert die Vorsorge und Dokumentation über den Bestand der digital genutzten Dienste die Situation von Erben, Angehörigen und Stellvertretern. Die Erben haben aufgrund der kurzen Ausschlagungsfristen nach § 1944 BGB insbesondere ein Interesse daran, bald nach dem Erbfall den Bestand des Nachlasses aufzuklären und mögliche Geschäftsbeziehungen abzuwickeln. Der Erblasser kann dies durch seine Vorsorge erleichtern, genauso wie er für den Fall der Hilfsbedürftigkeit Regelungen treffen kann, dass einerseits unnötig gewordene Verträge gekündigt und so Kosten erspart, andererseits wichtige Geschäftsbeziehungen weitergeführt werden können. Daneben kann auch ein Interesse der Angehörigen des Nutzers bestehen, dass sein Andenken geschützt sowie mit seinen Daten verantwortungsvoll umgegangen wird.[1]

Um diese Interessen zu wahren, hat der Nutzer verschiedene Vorsorgemöglichkeiten, die teilweise bereits zu Lebzeiten, teilweise erst mit dem Todesfall Wirkung entfalten. Diese Vorsorgemöglichkeiten werden nachfolgend im Hinblick auf ihre Geeignetheit im Rahmen des digitalen Bereichs untersucht. Auch wenn der Verbraucher eine Vorsorge getroffen hat, stellen sich weitere praktische Fragen dahingehend, wie Erben oder Bevollmächtigte ihre Begünstigung gegenüber den Dienstanbietern nachweisen und sich legitimieren können, um tatsächlich auf die digitalen Inhalte zugreifen zu können.

6.2 Rechtliche Vorsorgemöglichkeiten mit Wirkung zu Lebzeiten

Der Nutzer eines Online-Dienstes hat bereits zu seinen Lebzeiten die Möglichkeit, für den Fall vorzusorgen, dass er selbst seine Rechte und Pflichten nicht mehr wahrnehmen kann. Darauf ist insbesondere deshalb gesondert hinzuweisen, als der in der Diskussion ins Zentrum geratene Begriff des digitalen Nachlasses die ebenfalls bestehende Notwendigkeit, für lebzeitige Hilfsbedürftigkeit vorzusorgen, in den Hintergrund gerückt hat. Auch in dieser Situation besteht aber dasselbe Interesse, dass eine ausgewählte Person, welcher der Verbraucher Vertrauen entgegen bringt, die digitalen Dienste und Inhalte verwaltet.[2]

6.2.1 Vorsorgevollmacht

Eine Vorsorgevollmacht bietet sich besonders mit Wirkung bereits zu Lebzeiten an, wenn rasches Handeln erforderlich ist, oder der Betroffene nicht riskieren will, dass seine Angelegenheiten erst nach Durchführung eines gerichtlichen Betreuungsverfahrens besorgt werden, da eine Vorsorgevollmacht grundsätzlich mit dem Zeitpunkt ihrer Erstellung Wirksamkeit erlangt. Nicht empfehlenswert

[1] *Raude*, RNotZ 2017, S. 17 (24); *Steiner/Holzer*, ZEV 2015, S. 262 (265).
[2] *Raude*, RNotZ 2017, S. 17 (24).

sind Gestaltungen, nach denen die Vollmacht (im Außenverhältnis) erst nach Eintritt der Geschäftsunfähigkeit oder Betreuungsbedürftigkeit wirksam wird, da sich insoweit die eindeutige Feststellung und Beweisbarkeit des Eintritts der Bedingung im Rechtsverkehr als schwierig erweisen kann.[3]

Die Vollmacht kann insofern mit Wirkung allein zu Lebzeiten des Betroffenen oder als transmortale Vollmacht, also mit Wirkung über den Todeszeitpunkt hinaus, ausgestaltet werden. Eine transmortale Vollmacht bietet sich an, wenn die Abwicklung der digitalen Angelegenheiten auch nach dem Tod durch den Bevollmächtigten durchgeführt werden soll, weil dieser beispielsweise zugleich der Erbe oder Testamentsvollstrecker ist, aber bereits vor Eröffnung einer Verfügung von Todes wegen oder der Erteilung eines Erbscheins tätig werden soll.[4]

Der Betroffene kann entweder die digitalen Angelegenheiten als Unterpunkt in eine allgemeine Vollmacht aufnehmen oder eine eigene digitale Vollmacht erstellen,[5] wobei letztere keine Sonderform der Vorsorgevollmacht darstellt, sondern lediglich eine Vollmacht, die den digitalen Bereich zum Gegenstand hat.[6] Die Aufnahme des digitalen Nachlasses als gesonderten Unterpunkt in einer solchen Vollmacht ist nicht zwingend erforderlich, aber kann erfolgen, um das Bewusstsein für dessen Bedeutung zu stärken.[7] Zudem kann eine ausdrückliche Nennung der digitalen Angelegenheiten dazu dienen, die Akzeptanz der Vollmacht im Rechtsverkehr zu stärken.[8] Als Stellvertreter sollte eine Person gewählt werden, die das notwendige Verständnis für den Problemkreis und die erforderlichen technischen Kenntnisse aufweist.[9]

Die Erteilung einer Vorsorgevollmacht bedarf zwar keiner besonderen Form und könnte daher theoretisch auch mündlich erfolgen.[10] Allerdings sollte mindestens die Schriftform eingehalten, besser noch die notarielle Beurkundung durchgeführt werden. Dies ergibt sich einerseits daraus, dass eine Vorsorgevollmacht nur vorrangig vor der Anordnung einer Betreuung ist, wenn sie wirksam erteilt und im Zeitpunkt des Betreuungsverfahrens noch nicht erloschen ist. Bestehen Beweisschwierigkeiten hinsichtlich der wirksamen Ermächtigung, droht die Ersatzbestellung eines Betreuers. Insbesondere um den Nachweis der Geschäftsfähigkeit zu erbringen bzw. Zweifel dahingehend auszuräumen, ist die notarielle Form der Urkunde zu empfehlen. Der Vollmachtgeber muss für die Erteilung der Vollmacht zumindest eine partielle Geschäftsfähigkeit in dem Sinne aufweisen, als er verstehen kann, dass für den Fall seiner Handlungsunfähigkeit eine andere Person die Aufgaben für ihn wahrnimmt und welche Risiken dies bergen kann.[11] Auch wenn die Rechtsprechung dazu neigt, im Zweifel die

[3] *Kropp*, FPR 2012, S. 9; *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (20 f.).
[4] *Raude*, RNotZ 2017, S. 17 (24).
[5] *Raude*, RNotZ 2017, S. 17 (24); *Gloser*, MittBayNot 2016, S. 101 (103), hält eine Erweiterung der bestehenden Muster für General- und Vorsorgevollmachten für entbehrlich.
[6] *Steiner/Holzer*, ZEV 2015, S. 263 (265).
[7] *Salomon*, NotBZ 2016, S. 324 (330).
[8] *Herzog/Pruns*, Digitaler Nachlass, S. 158; *Pruns*, ErbR 2018, S. 614 (621).
[9] *Steiner/Holzer*, ZEV 2015, S. 263 (265).
[10] Mit Ausnahme der §§ 1905 V 2, 1906 V 1 BGB oder wenn in Ausnahme zu § 167 II BGB für die Veräußerung eines Grundstücks die grundbuchrechtliche Form erforderlich ist, § 29 I GBO, vgl. dazu *BGH*, NJW 2016, 1516.
[11] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (21).

Wirksamkeit von Vollmachten zu bejahen,[12] gehen diese Zweifel doch stets zu Lasten der effektiven Tätigkeit des Bevollmächtigten, wenn die Vollmacht im Rechtsverkehr nicht oder nicht ohne Einwände anerkannt wird.[13] Auch im (ausländischen) Rechtsverkehr – die Dienstanbieter haben ihren Sitz häufig nicht in Deutschland – ist hinsichtlich der Akzeptanz der Vorsorgevollmacht die notarielle Form empfehlenswert.[14] Zudem kann die notariell beurkundete Vorsorgevollmacht zusätzlich beim elektronischen Zentralen Vorsorgeregister der Bundesnotarkammer (§ 78a I BNotO, § 20a BeurkG) hinterlegt werden. Dabei erfolgt ein Auskunftsersuchen aber nur durch Gerichte, vgl. § 78b I 1 BNotO i. V. m. § 6 Vorsorgeregister-Verordnung – VRegV, da Sinn und Zweck der Regelung die Information der Gerichte zur Vermeidung nicht erforderlicher Betreuungen ist.[15] Geschäftspartner des Vollmachtgebers können selbst keine Einsicht in das Register nehmen, sondern gegebenenfalls nur Auskunft bei Gericht ersuchen.

Im Rahmen der Erteilung ist wie stets einerseits darauf zu achten, dass bei einer weit gefassten Vollmacht eine Ausübung gegen den Willen des Vollmachtgebers möglich ist. Andererseits muss die Vorsorgevollmacht so gefasst sein, dass sie das konkrete Vertretungsbedürfnis umfassend erfasst und gegenständlich sowie sachlich abdeckt, um die ergänzende Anordnung einer rechtlichen Betreuung zu vermeiden[16] und ausreichende Akzeptanz im Rechtsverkehr sicherzustellen. Besonders im Außenverhältnis bietet sich daher eine möglichst unbeschränkte Geltung.[17] Daneben kann der Nutzer dem Stellvertreter im Außenverhältnis aber auch im Sinne einer Vorsorgeverfügung nur einzeln festgelegte rechtsgeschäftliche Handlungen übertragen. Der Stellvertreter hat dann keinen Ermessenspielraum, sondern nur die Aufgabe, die Durchsetzung der vorher festgelegten Entscheidungen im Vorsorgefall sicherzustellen. So könnte der Nutzer den Stellvertreter allein dazu ermächtigen, eine bestimmte Online-Vertragsbeziehung für den Fall seiner Geschäftsunfähigkeit zu kündigen. Dieser Gestaltung wird jedoch vorgeworfen, dass sie zu unflexibel sei, da spätere Willensänderungen oder Veränderungen auf tatsächlicher Ebene nicht berücksichtigt werden könnten und zudem dadurch tatsächlich nur der geregelte Fall von der Bevollmächtigung erfasst sei.[18]

Insofern muss der Vollmachtgeber nach seiner Interessenlage abwägen, ob er eine möglichst umfassende Stellvertretung für alle digitalen Angelegenheiten möchte, oder nur eine bestimmte Angelegenheit erledigt werden soll. Insbesondere in letzterem Fall ist auch eine Vorsorgeverfügung mit beschränktem Umfang möglich. Der Betroffene kann grundsätzlich auch für verschiedene digitale Angelegenheiten verschiedene Vorsorgebevollmächtigte bestellen. Dabei ist darauf zu achten, dass die Vorsorgevollmacht so präzise gefasst ist, dass es einerseits nicht zu ungewollten Kompetenzüberschneidungen der Vorsorgebevollmächtigten kommt und andererseits die Vollmacht von dem jeweiligen Vertragspartner auch akzeptiert wird.

[12] Statt aller BGH, NJW 2016, 1514; OLG München, FamRZ 2010, 756 ff.
[13] Auf dieses Problem ebenfalls hinweisend *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 54; dazu auch OLG München, FamRZ 2009, 2033.
[14] *Steiner/Holzer*, ZEV 2015, S. 263 (265).
[15] *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 20a Rn. 12 f.
[16] *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 227.
[17] *Raude*, RNotZ 2017, S. 17 (24).
[18] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (19 f.).

Ist aber eine allgemeine (General-)Vorsorgevollmacht erteilt, kann der Nutzer, um einem unkontrollierten Schalten und Walten des Bevollmächtigten entgegenzuwirken, im Innenverhältnis – je nach Interessenlage des Vollmachtgebers – möglichst konkrete Anweisungen erteilen. So kann im Innenverhältnis die beschränkende Anweisung aufgenommen werden, erst bei Eintritt des Vorsorgefalls (z. B. ärztlich festgestellter Eintritt der Hilfsbedürftigkeit) von der Vollmacht Gebrauch zu machen.[19] Daneben können Anweisungen dahingehend erteilt werden, wie mit bestimmten Daten oder Vertragsverhältnissen im Vorsorgefall zu verfahren ist.[20] Dem Bevollmächtigten können beispielsweise Anweisungen gegeben werden, bestimmte Vertragsverhältnisse zu kündigen, nach den Vorgaben des Vollmachtgebers weiterzuführen oder rein private Daten sofort zu löschen.

Dabei muss der Vollmachtgeber entscheiden, ob diese Anweisungen direkt in das Vollmachtdokument aufgenommen werden sollen oder in einem separaten Dokument bzw. einer Anlage nur dem Bevollmächtigten selbst mitgeteilt werden. Befinden sich die Anweisungen im selben Dokument, können theoretisch alle Geschäftspartner im Rechtsverkehr, denen die Vollmacht vorgelegt wird, von den Anweisungen im Innenverhältnis Kenntnis erlangen. Insbesondere, wenn im Außenverhältnis eine allgemeine (General-)Vorsorgevollmacht erteilt wurde, empfiehlt sich daher die Trennung von Vollmacht und Anweisung im Innenverhältnis.[21]

Als Kontrollinstrument besteht auch die Möglichkeit, dass der Vollmachtgeber einen zweiten oder mehrere Vorsorgebevollmächtigte bestellt, denen die Aufgabe der Überwachung des ersten Vorsorgebevollmächtigten zufällt.[22] Missbraucht der Vorsorgebevollmächtigte seine Befugnisse kann der Überwachungsbevollmächtigte kontrollierend und schützend zum Wohl des Vollmachtgebers eingreifen. Befürchtet der Vollmachtgeber zudem, dass der Bevollmächtigte sein Amt bei Eintritt des Vorsorgefalls oder über die notwendige Dauer nicht ausüben kann, besteht auch die Möglichkeit einen oder mehrere Ersatzbevollmächtigte zu bestellen, die für den Fall des Wegfalls des Stellvertreters tätig werden sollen.

Der Vollmachtgeber sollte zudem dem Bevollmächtigten den Bestand der digitalen Angelegenheiten mit allen relevanten Zugangsdaten zugänglich machen. Andernfalls muss der Bevollmächtigte im Vorsorgefall erst einmal herausfinden, welcher Datenbestand vorhanden ist und gegebenenfalls die Herausgabe der Zugangsdaten von den Dienstanbietern verlangen. Zwar steht nach deutschem Rechtsverständnis dem Vorsorgebevollmächtigten gegen die Dienstanbieter ein Auskunftsanspruch hinsichtlich der Zugangsdaten und Passwörter zu. Allerdings kann sich die Durchsetzung dann als schwierig erweisen, wenn der Dienstanbieter seinen Sitz im Ausland hat und diese Rechtsordnung beispielsweise die transmortale Vollmacht nicht kennt oder dort Verbraucherrechte weniger geschützt sind. Durch Hinterlegung der erforderlichen Zugangsdaten kann dann sichergestellt werden, dass der Bevollmächtigte im Ernstfall ohne Probleme und vorherige Auseinandersetzung mit dem Dienstanbieter auf diese zugreifen kann.[23]

[19] *Kropp*, FPR 2012, S. 9 (10).

[20] *Raude*, RNotZ 2017, S. 17 (24); mit konkreten Beispielen für Handlungsanweisungen *Salomon*, NotBZ 2016, S. 324 (330 f.).

[21] *Raude*, RNotZ 2017, S. 17 (24).

[22] *Löhnig*, Probleme der Vorsorgevollmacht nach deutschem Recht, in: Löhnig/Schwab (Hrsg.), Vorsorgevollmacht, S. 15 (25).

[23] *Raude*, RNotZ 2017, S. 17 (26); *Gloser*, MittBayNot 2016, S. 101 (103) hält demgegenüber eine Aufzählung aller Online-

6.2.2 Betreuungsverfügung

Die Betreuung wird zwar gerichtlich angeordnet, für den Fall, dass der Betroffene keine private Vorsorge getroffen hat. Allerdings kann der Betroffene zumindest insoweit Einfluss nehmen, als er gemäß § 1897 IV BGB vor oder während des Betreuungsverfahrens vorschlagen kann, dass eine bestimmte natürliche, volljährige Person zum Betreuer bestellt wird (S. 1) oder dass eine Person nicht zum Betreuer bestellt werden soll (S. 2). Die erste Möglichkeit ist dabei für das Gericht grundsätzlich bindend und dem Vorschlag des Betroffenen zu folgen, wenn nicht dessen Wohl entgegensteht.[24] Daneben kann der Betroffene auch Wünsche bezüglich der inhaltlichen Ausgestaltung des Betreuungsverhältnisses äußern, die für den Betreuer bindend sind.[25] Dies gilt unabhängig von der Geschäfts- oder Einsichtsfähigkeit des Betroffenen oder der Dauerhaftigkeit des Wunsches.[26] Dieser muss nur im Zeitpunkt der Betreuerbestellung vorliegen, was sich bereits aus § 1897 IV 3 BGB ergibt[27] und kann auch noch im gerichtlichen Verfahren ausgedrückt werden.

Möchte der Betroffene somit, dass eine von ihr gewählte Person das Amt des Betreuers übernimmt, kann er eine solche auch für seine digitalen Angelegenheiten vorschlagen.

6.3 Trans- oder postmortale Vollmacht als rechtliche Vorsorgemöglichkeit mit Wirkung im Todesfall

Eine Vollmacht kann aber auch zu dem Zweck erteilt werden, dass eine dritte Person im Todesfall den digitalen Nachlass für den Erblasser verwaltet. Dies ist dann zu empfehlen, wenn der Bevollmächtigte bereits vor Eröffnung der Verfügung von Todes wegen oder der Erteilung eines Erbscheins von seiner Vollmacht Gebrauch machen können soll.[28] Dabei kann in der Vollmacht bestimmt werden, dass ihre Wirksamkeit erst im Todeszeitpunkt eintritt (postmortale Vollmacht). Daneben besteht – wie oben bereits beschrieben – auch die Möglichkeit, die Vollmacht als transmortale Vollmacht zu erteilen, also mit Wirkung bereits zu Lebzeiten über den Todeszeitpunkt hinaus. Auch die Erteilung einer nach oder über den Tod hinaus wirkenden Vollmacht ist unabhängig von einer Erbenstellung des Bevollmächtigten. Daher unterliegt eine derartige Vorsorgevollmacht ebenfalls keinen – auch nicht den erbrechtlichen – Formvorschriften und könnte daher gegebenenfalls auch mündlich erteilt werden. Aus Gründen der Beweisbarkeit und Akzeptanz im Rechtsverkehr ist jedoch mindestens Schriftform, besser noch die notarielle Beurkundung zu empfehlen.[29]

Hinsichtlich der inhaltlichen Ausgestaltung und der zur Verfügung zu stellenden Zugangsdaten gilt das bereits in Kapitel 6.2.1 auf Seite 176 zur Vorsorgevollmacht Beschriebene.

Konten in der Vollmacht eher für verwirrend, insbesondere wenn sich der Datenbestand noch verändern kann.

[24] *BayObLG*, NJWE-FER 2001, 234; BGH, NJW 2010, 3777 (3778).

[25] *Roth*, in: Dodegge/Roth (Hrsg.), BtKomm, Kap. C Rn. 163.

[26] BGH, NJW 2011, 925 (925 f.).

[27] BGH, NJW-RR 2011, 1507 (1509).

[28] *Raude*, RNotZ 2017, S. 17 (24).

[29] Siehe dazu bereits oben.

Nach dem Tod des Erblassers vertritt der Bevollmächtigte die Erben als Rechtsnachfolger des Erblassers.[30] Problematisch an der Erteilung einer Vollmacht ist jedoch, dass die Erben die Vollmacht jederzeit frei widerrufen können. Dies gilt gemäß § 168 S. 2 BGB unabhängig davon, ob auch das zugrundeliegende Rechtsverhältnis (z. B. Auftrag) endet.[31] So können die Erben den Stellvertreter aus seinem Amt entfernen und den Willen des Erblassers vereiteln.

Zwar kann die Vollmacht als unwiderrufliche Vollmacht erteilt werden. Allerdings nur, wenn es sich nicht um eine Generalvollmacht handelt, da eine unwiderrufliche Generalvollmacht die Privatautonomie des Vollmachtgebers zu sehr einschränken würde.[32] Nur Spezialvollmachten können also als unwiderruflich ausgestaltet sein. Zudem wird für den Ausschluss der Widerruflichkeit nach überwiegender Ansicht eine besondere Rechtfertigung und ein dem Interesse des Vollmachtgebers mindestens gleichwertiges Interesse des Bevollmächtigten oder eines Dritten an dem Vertretergeschäft verlangt.[33] Im Rahmen des digitalen Nachlasses wird infrage gestellt, ob dieses erforderliche Interesse des Bevollmächtigten oder eines Dritten bejaht werden kann, oder ob nicht allein der Erblasser als Dateninhaber ein Interesse an der Unwiderruflichkeit hat.[34] Selbst wenn man die Unwiderruflichkeit bejaht, bleibt aber die Möglichkeit des Widerrufs aus wichtigem Grund, beispielsweise dann, wenn das zugrunde liegende Kausalverhältnis erlischt, vgl. § 168 S. 1 BGB (für den Auftrag vgl. § 671 III BGB).[35] Die Gefahr, dass der Stellvertreter von den Erben aus seinem Amt entfernt wird, lässt sich somit nicht gänzlich ausschließen.

6.4 Gestaltungsmöglichkeiten von Todes wegen

Nutzer können auch von Todes wegen über ihren digitalen Nachlass verfügen. In diesem Zusammenhang wird häufig von der Errichtung eines „digitalen Testaments“ gesprochen. Insoweit ist darauf hinzuweisen, dass lediglich der Regelungsgegenstand der Verfügung digital ist. Es handelt sich nicht um eine Sonderform einer letztwilligen Verfügung. Somit sind die gesetzlichen Formvorschriften für die Errichtung eines Testaments, also eigenhändig (§ 2247 BGB) oder notariell (§ 2232 BGB), einzuhalten.[36]

Trifft der Nutzer keine Vorsorge, geht im Fall seines Todes sein gesamtes Vermögen und damit auch sein digitaler Nachlass auf seine gesetzlichen Erben gemäß §§ 1924 ff. BGB über, die zusammen eine Erbengemeinschaft bilden, § 2032 BGB. Dies bedeutet, dass sämtliche Erben in die digitalen Inhalte

[30] *Seidler*, Digitaler Nachlass, S. 155.
[31] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 168 Rn. 16.
[32] *Schilken*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 168 Rn. 9; *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 168 Rn. 25.
[33] *Schilken*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 168 Rn. 8; *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 168 Rn. 20.
[34] *Seidler*, Digitaler Nachlass, S. 156.
[35] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 168 Rn. 29.
[36] *Seidler*, Digitaler Nachlass, S. 150 f.; *Gloser*, MittBayNot 2016, S. 101 (104); *Herzog/Pruns*, Digitaler Nachlass, S. 160; *Bräutigam* in: Burandt/Rojahn (Hrsg.), Erbrecht, § 1922 BGB Anhang. Digitaler Nachlass Rn. 28; *Herzog* in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 82.

Einsicht nehmen und somit auch von persönlichen Informationen des Erblassers Kenntnis erhalten können sowie bei Weiternutzung gemeinsam in den Vertrag eintreten.

Entspricht dies nicht dem Willen des Erblassers, muss er tätig werden. Dabei kann der Erblasser unterschiedliche Gestaltungsziele verfolgen, beispielsweise nur bestimmten Personen Zugriff auf den digitalen Nachlass gewähren, verschiedene digitale Nachlassgegenstände unterschiedlichen Personen zuwenden oder nach seinem Tod einen Zugriff gänzlich verhindern. Hierzu stehen ihm sämtliche erbrechtlichen Gestaltungsmöglichkeiten zur Verfügung.

6.4.1 Verweigerung des digitalen Nachlasses

Denkbar ist, dass es dem Wunsch des Erblassers entspricht, nach seinem Tod den Zugriff auf seinen digitalen Nachlass oder bestimmte Teile hieraus gänzlich zu verhindern. So kann ein bestimmter Datenträger besonders private Bilder oder E-Mails enthalten, in welche die Erben keine Einsicht nehmen sollen. Dabei bestehen einerseits rechtliche Möglichkeiten, wie dies erreicht werden kann. Andererseits könnte die Einsichtnahme auch durch technische Mittel vereitelt werden.

6.4.1.1 Erbrechtliche Möglichkeiten

Begehrt der Erblasser im Fall seines Todes die Löschung aller oder lediglich bestimmter Benutzerkonten und/oder (der dazugehörigen) Daten, ohne dass die Erben vorher Einsicht nehmen, reicht allein die Geheimhaltung der Zugangsdaten nicht immer aus. Die Erben haben die Möglichkeit, einen Auskunftsanspruch gegen den Dienstanbieter geltend zu machen, mit der Folge, dass dieser die Zugangsdaten im Fall des Nachweises der Erbberechtigung herauszugeben hat.[37] Somit können die Erben den Willen des Erblassers vereiteln.

Mithilfe einer Auflage in der letztwilligen Verfügung kann der Erblasser die Erben aber verpflichten, Vertragsbeziehungen zu kündigen und eine (vorherige) Einsichtnahme in die Nutzerkonten oder Speichermedien zu unterlassen.[38] Fallen den Erben die Daten zusammen mit dem Speichermedium oder der Vertragsbeziehung zu, kann mit der Zuwendung eine Auflage verbunden werden, gewisse Datenbestände zu löschen.[39] Da der Erblasser jedoch die Erfüllung der Auflage nach seinem Tod nicht mehr selbst kontrollieren kann, ist es empfehlenswert, diese weiter abzusichern.

Zudem gilt in dem Fall, dass ein Dienstanbieter – ausnahmsweise berechtigt[40] – zum Nachweis des Erbrechts die Vorlage eines Erbscheins verlangt, in welchem bestehende Auflagen nicht vermerkt werden.[41] Insoweit könnte beispielsweise eine Auflage zur Löschung eines Nutzerkontos für sich genommen wirkungslos sein, wenn der Dienstanbieter von dieser nicht erfährt und dem Erben Zugriff gewährt.

[37] *Gloser*, MittBayNot 2016, S. 101 (107).
[38] *Seidler*, Digitaler Nachlass, S. 153.
[39] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 365 f.
[40] Siehe dazu ausführlich in Kapitel 6.6.2 auf Seite 232.
[41] *Grziwotz* in: Säcker u. a. (Hrsg.), MükoBGB, § 2353 Rn. 43.

Um dem Willen des Erblassers Geltung zu verschaffen, könnte daher einerseits durch technische Mittel der Zugriff verhindert werden.[42]

Aus rechtlicher Sicht besteht daneben die Möglichkeit, Testamentsvollstreckung anzuordnen und so eine Überwachung der Erben zu erreichen.[43] Der Testamentsvollstrecker würde dann mit der Aufgabe betraut, zu kontrollieren, ob die Erben die Löschung ohne vorherige Einsicht vorgenommen haben.

Eine einfachere Möglichkeit, die auch gewährleisten kann, dass die Erben keinen Zugriff auf die Daten nehmen können, ist, einen Testamentsvollstrecker oder Vorsorgebevollmächtigten mit der Löschung bestimmter Daten oder der Kündigung gewisser Vertragsverhältnisse zu betrauen.[44]

Insbesondere die Anordnung einer Testamentsvollstreckung ist im vorliegenden Fall geeignet. Zunächst kann der Testamentsvollstrecker zur Verwaltung des Nachlasses gemäß der konkreten Anordnungen des Erblassers bestellt werden, vgl. §§ 2205, 2216 BGB. Die Verwaltungsanordnungen können dabei auch darauf gerichtet sein, dass der Testamentsvollstrecker bestimmte Benutzerkonten und/oder Daten bzw. Datenordner löschen soll.[45] Da der Testamentsvollstrecker eine Vertretungs- und Verfügungsbefugnis hat, ist er auch befugt, Online-Vertragsverhältnisse zu kündigen. Zudem unterliegen die Erben bei Anordnung der Testamentsvollstreckung gemäß § 2211 BGB einer Verfügungsbeschränkung, sodass auf diese Weise der Zugriff der Erben auf die zu löschenden Daten verhindert werden kann.[46] Bei der Durchführung dieser Handlungen ist der Testamentsvollstrecker zudem zur Verschwiegenheit verpflichtet.[47] Dabei kann auch dem Testamentsvollstrecker aufgegeben werden, keine Einsicht in die betreffenden Datenbestände zu nehmen. Zum Testamentsvollstrecker sollte insofern eine vertrauenswürdige Person bestellt werden. Dies kann entweder eine Person sein, die der Erblasser persönlich kennt und der er Vertrauen entgegenbringt, oder ein Berufsträger (beispielsweise ein Rechtsanwalt), der zudem besonderen beruflichen Regeln unterliegt.

6.4.1.2 Technische Möglichkeiten

Zu den Vorsorgemöglichkeiten gehört auch die Option des Erblassers, eine Weitergabe des digitalen Nachlasses ganz oder in Teilen zu verhindern. Der Erblasser könnte – falls von den Dienstanbietern unterstützt (vgl. Googles Kontoinaktivität-Manager) – den betreffenden Online-Dienst zu Lebzeiten so konfigurieren, dass das Nutzerkonto mitsamt aller Daten nach Meldung oder Erkennung des Sterbefalls gelöscht wird. Alternativ kann der Erblasser zu Lebzeiten einen digitalen Nachlassdienst beauftragen, im Sterbefall bestimmte Konten oder Daten zu löschen. Einige digitale Nachlassdienste kooperieren mit den wichtigsten Online-Dienstanbietern und nehmen vom Erblasser auch Löschaufträge für Daten an, von denen die Erben nichts erfahren sollen, siehe Kapitel 6.5.5 auf Seite 205.

[42] Siehe hierzu sogleich.
[43] *Gloser*, MittBayNot 2016, S. 101 (107); *Raude*, RNotZ 2017, S. 17 (27).
[44] Die Vor- und Nachteile der Vorsorgevollmacht gegenüber der Testamentsvollstreckung sind in Kapitel 6.4.4.2 auf Seite 191 ausführlich dargestellt.
[45] *Gloser*, MittBayNot 2016, S. 101 (107); *Biermann* in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 77.
[46] *Raude*, RNotZ 2017, S. 17 (26).
[47] *Schleifenbaum*, ErbR 2015, S. 230 (236).

Alternativ könnte der Erblasser eine ausgewählte Vertrauensperson anweisen, im Sterbefall nach einem regulären Login die Konten und Daten löschen zu lassen. Dabei kann allerdings nicht garantiert werden, dass die Vertrauensperson einer solchen Verpflichtung auch wirklich nachkommt und anschließend die korrekte Umsetzung kontrolliert wird, vgl. das Kapitel 4.2 auf Seite 103. Sicherer wäre es, wenn der Erblasser selbst noch zu Lebzeiten die Löschung vornehmen könnte. In der Praxis ist der dafür geeignete Zeitpunkt schwierig zu bestimmen und die Durchführung evtl. persönlich sehr belastend.

Eine Alternative zur Datenlöschung besteht darin, die Daten grundsätzlich zu verschlüsseln und die Weitergabe der Schlüssel und Passwörter zu verhindern. Dies kann allerdings technisch anspruchsvoll sein und bietet dennoch keinen absoluten Schutz gegen spätere Zugriffe. Viele Betriebssysteme bieten passwortgeschützte Festplattenverschlüsselung an. Zudem gibt es spezielle Softwarelösungen, mit denen Dateien, Ordner, Festplattenpartitionen oder Wechseldatenträger verschlüsselt werden können. Viele Anwendungsprogramme (z. B. Zip-Komprimierungsprogramme) bieten Funktionen zur Verschlüsselung der von ihnen erzeugten Dateien an, oft mithilfe eines symmetrischen Schlüssels, der mit einem selbst gewählten Passwort geschützt ist. Passwörter sind allerdings während der Eingabe nicht unbedingt gegen Ausspähen sicher.[48] Eine Verschlüsselung bietet einen gewissen Schutz zumindest im abgeschalteten Zustand des Systems, also bei Verlust, Diebstahl oder auch bei Hinterlassung des Datenträgers im Sterbefall, solange das angewendete Verschlüsselungsverfahren als sicher gilt und Schlüssel und Passwörter von den verschlüsselten Daten getrennt und unzugänglich aufbewahrt werden. Die Sicherheit der Verschlüsselung kann durch den Einsatz spezieller Hardware gesteigert werden, beispielsweise durch die Speicherung des Schlüssels auf einer separaten Chipkarte oder einem Sicherheitstoken oder durch die Nutzung externer Datenträger (USB-Sticks, USB-Festplatten), die mit einer eigenen Verschlüsselungskomponente ausgestattet sind.

Theoretisch kann aber jede Verschlüsselung auch ohne Kenntnis des Schlüssels durch Ausprobieren sämtlicher möglicher Schlüssel (sogenannte Brute-Force-Angriffe) gebrochen werden. Als hinreichend sicher gelten solche Verschlüsselungsverfahren und Schlüssellängen, bei denen ein derartiger Versuch auch bei hochleistungsfähigen und ggf. vernetzten Rechnern nur in übermäßig viel Zeit erfolgreich sein könnte. Verschlüsselung gilt damit praktisch dann als sicher, wenn sie durch die bekannten Angriffsverfahren und mit den verfügbaren Ressourcen in vertretbarer Zeit nicht gebrochen werden kann. Weil Computer immer leistungsfähiger werden und auch das Wissen über mathematische Algorithmen zunimmt, können Verfahren und Schlüssellängen, die heute noch als sicher gelten, in wenigen Jahren schon unsicher sein. Bewahren also ggf. die Erben den verschlüsselten Datenträger lang genug auf, so könnte gegen den Willen des Erblassers doch noch ein Zugriff auf die Daten erfolgen. Die Erben könnten umgehend einen IT-Dienstleister damit beauftragen, die auf den Datenträgern vorhandenen Daten zu sichern und einen ggf. vorhandenen Passwortschutz zu entfernen.

Für den Fall, dass der Erblasser den Zugriff auf lokale Daten verhindern möchte, sollten die Daten im Sterbefall durch eine ausgewählte Vertrauensperson oder einen Bevollmächtigten gelöscht werden. Einfache Löschfunktionen löschen allerdings nur die Verweise auf eine Datei im Inhaltsverzeichnis

[48] Beispielsweise durch „Keylogger“-Programme, die Tastatureingaben aufzeichnen können, durch Auslesen des Hauptspeichers, durch Ausprobieren möglicher Passwörter usw.

des Datenträgers. Mithilfe leicht zugänglicher Hilfsprogramme können die vermeintlich entfernten Daten wieder hergestellt werden. Um dies zu erschweren, können spezielle Löschprogramme eingesetzt werden. Diese verhindern die Rekonstruktion gelöschter Daten, indem sie einen Datenträger mehrfach mit unterschiedlichen Daten überschreiben. Aber auch dadurch ist kein absolut sicheres Löschen gewährleistet. Viele Speichermedien verwenden komplizierte Mechanismen, um auftretende Fehler zu beherrschen, unterbinden damit aber auch das direkte Löschen von Daten durch Überschreibprogramme. Auch durch Formatieren des Datenträgers werden die vorhandenen Daten nicht unbedingt überschrieben, sodass evtl. eine Rekonstruktion der Daten möglich bleibt. Verschlüsseln und Löschen der Daten sind keine wirkliche Alternative zur physischen Vernichtung (z. B. Schreddern) der Datenträger.[49]

6.4.1.3 Fazit

Für lokal aufbewahrte verschlüsselte Festplatten, Ordner und Dateien kann ein dauerhafter Schutz der Daten gegen Zugriffe nicht allein durch Verschlüsselung gewährleistet werden, auch dann nicht, wenn der Entschlüsselungsschlüssel vorsorglich vernichtet wurde. Auch das Löschen der Daten garantiert nicht, dass die Daten nicht wieder hergestellt werden können. Für den Fall, dass der Erblasser den Zugriff auf lokale Daten verhindern möchte, gibt es keine wirkliche Alternative zur physischen Vernichtung der entsprechenden Datenträger.

Zu empfehlen ist daher entweder die physische Vernichtung von Datenträgern oder rechtlich die Einsetzung eines Testamentsvollstreckers, der Datenbestände löscht, ggf. verbunden mit der Auflage an die Erben, nach der Löschung nicht zu versuchen, die Daten wiederherzustellen.

6.4.2 Auswahl der Erben/Begünstigten

Möchte der Erblasser seinen digitalen Datenbestand vererben, hat er zunächst die Möglichkeit, durch ein Testament einen Alleinerben oder beliebig viele Erben als seine Rechtsnachfolger, § 1937 BGB, und somit auch als Erben seines gesamten digitalen Nachlasses einzusetzen. Mehrere Erben bilden auch hier eine Erbengemeinschaft im Sinne des § 2032 BGB, sodass sämtliche Erben berechtigt sind, gemeinsam Einsicht in Benutzerkonten zu nehmen und diese zu nutzen. Insoweit wird vorgeschlagen, in der letztwilligen Verfügung klarstellend darauf hinzuweisen, dass die Universalsukzession auch den digitalen Nachlass umfasst.[50] Dies kann zwar aufgrund der bestehenden Rechtsunsicherheiten Rechtssicherheit schaffen. Allerdings kann es sich hierbei stets nur um eine deklaratorische Regelung handeln, da hinsichtlich des digitalen Nachlasses keine Sondererbfolge besteht, was auch in der letztwilligen Verfügung zum Ausdruck kommen sollte.[51]

[49] Zur Problematik des „endgültigen Löschens“ siehe auch die BSI-Seite https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html

[50] *Steiner/Holzer*, ZEV 2015, S. 262 (266); *Pruns*, ErbR 2018, S. 614 (621).

[51] *Herzog/Pruns*, Digitaler Nachlass, S. 161; *Pruns*, ErbR 2018, S. 614 (621).

6.4.2.1 Vor- und Nacherbschaft

Möchte der Erblasser über längere Zeit bestimmen, wem sein digitaler Nachlass zufällt, kann grundsätzlich auch eine Vor- und Nacherbfolge gemäß §§ 2100 ff. BGB angeordnet werden. Allerdings ist fraglich, inwiefern diese hinsichtlich des digitalen Nachlasses sinnvoll erscheint. Zunächst kann allein durch die Bestimmung von Vor- und Nacherben keine Sondererbfolge in dem Sinne generiert werden, dass verschiedenen Personen unterschiedliche digitale Nachlassgegenstände zufallen. Im Erbrecht gilt ein Typenzwang dahingehend, dass der Erblasser nicht ohne Weiteres einzelne Gegenstände mit dinglicher Wirkung an bestimmte Personen vererben und somit eine Sondererbfolge generieren kann.[52] Nach dem Grundsatz der Universalsukzession kann so der digitale Nachlass nur als Ganzes zunächst auf Vor- und anschließend auf Nacherben übergehen.

Zudem unterliegt der Vorerbe hinsichtlich des digitalen Nachlasses keinen Beschränkungen im Sinne der §§ 2112–2115 BGB, da es sich hinsichtlich der Online-Vertragsbeziehungen um rein schuldrechtliche Vertragsbeziehungen handelt, über die auch der Vorerbe frei verfügen kann.[53] Auch hinsichtlich des Eigentums an lokalen Speichermedien bestehen keine Beschränkungen. So könnte der Vorerbe beispielsweise die Vertragsbeziehungen kündigen oder Daten von lokalen Speichermedien löschen, wenn er an diesen kein Interesse hat. Zudem besteht das rein praktische Problem, dass der Vorerbe berechtigt ist, Zugangsdaten und vor allem Passwörter zu ändern. Kooperieren Vor- und Nacherbe nicht, müsste der Nacherbe somit zunächst einen Auskunftsanspruch gegen den Dienstanbieter geltend machen. Denkbar wäre nur, dass die Vorerbschaft mit einer Auflage im Sinne der §§ 1940, 2191 ff. BGB verbunden wird. Gegenstand einer Auflage kann eine Leistung, also jedes Tun oder Unterlassen sein, die auch Gegenstand eines Schuldverhältnisses sein kann.[54] Der Vorerbe könnte also verpflichtet werden, Daten nicht zu löschen oder Online-Vertragsbeziehungen für den Nacherben aufrecht zu erhalten.

6.4.2.2 Ersatzerbschaft

Befürchtet der Erblasser, dass ein (Allein-)Erbe vor dem Erbfall verstirbt oder die Erbschaft ausschlägt, kann er zudem einen oder mehrere Ersatzerben im Sinne des § 2096 BGB mittels letztwilliger Verfügung einsetzen. Insofern kann der Erblasser auch die Reihenfolge bestimmen, in der die Ersatzerben berufen sein sollen.

6.4.2.3 Teilungsanordnung und Vorausvermächtnis

Zwar kann der Erblasser aufgrund des Typenzwangs nicht ohne Weiteres einzelne Nachlassgegenstände mit dinglicher Wirkung an bestimmte Personen vererben.[55] Möchte der Erblasser aber gerade erreichen, dass verschiedenen Personen unterschiedliche digitale Nachlassgegenstände zufallen,

[52] *Leipold*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1937 Rn. 10.
[53] *Lieder*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2112 Rn. 1.
[54] *Weidlich*, in: Palandt (Hrsg.), BGB, § 2192 Rn. 3.
[55] *Leipold*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1937 Rn. 10.

besteht die Möglichkeit, mit schuldrechtlicher Wirkung durch Teilungsanordnung, § 2048 BGB,[56] oder (Voraus-)Vermächtnis, §§ 1939, 2147 ff. BGB,[57] zu bestimmen, dass einer Person ein bestimmter Nachlassgegenstand zugeordnet werden soll.

Ist der Begünstigte hinsichtlich bestimmter Datenbestände zugleich Erbe, kann einerseits eine Erbeinsetzung einer oder mehrerer Personen mit einer Teilungsanordnung erfolgen, § 2048 BGB, oder einzelnen Erben ein Vorausvermächtnis, § 2150 BGB, zugewendet werden. Zwar können nicht die Daten an sich bestimmten Personen zugeordnet werden. Allerdings kann gesteuert werden, wem diese zufallen, indem ein lokales Speichermedium mit den darauf befindlichen Daten oder die entsprechende Online-Vertragsbeziehung übertragen wird.

Im Rahmen eines Vermächtnisses kann stets nur ein Vermögensvorteil zugewendet werden. Dies ist bei Zuwendung eines Speichermediums unproblematisch der Fall. Bei Eintritt in eine Vertragsbeziehung liegt diese Voraussetzung jedenfalls dann vor, wenn der Vertrag nicht kostenpflichtig ist, da die Zugriffsmöglichkeit auf die Daten ein Vermögensvorteil sein kann. Im Rahmen der Verfügung sollte auch nicht nur das Speichermedium oder die Vertragsbeziehung übertragen werden, sondern in jedem Fall ein klarstellender Hinweis erfolgen, dass sich die Berechtigung auch auf die dazugehörigen Daten erstreckt, um Missverständnisse zu vermeiden.[58]

Auch durch eine Teilungsanordnung kann erreicht werden, dass nur bestimmte Erben berechtigt sein sollen, auf die Daten zuzugreifen. Allerdings erfolgt im Rahmen einer Teilungsanordnung eine Anrechnung des Werts des digitalen Nachlasses auf den Erbteil, die möglicherweise nicht gewünscht ist.[59] Zudem können sich hinsichtlich des Anrechnungswertes des digitalen Nachlasses Bewertungsschwierigkeiten ergeben. Soll der digitale Nachlasswert aber als vermögenswerte Begünstigung des Zuwendungsempfängers vermacht werden, bietet sich ein Vorausvermächtnis an, bei dem der Erbe den Wert des Vermächtnisses zusätzlich zu seinem Erbteil erhält.

Hinsichtlich der Teilungsanordnung ist darüber hinaus zu beachten, dass der begünstigte Erbe die Rechtsposition erst im Rahmen der Auseinandersetzung der Erbschaft tatsächlich erhält, da der Anspruch aus § 2048 BGB erst zu diesem Zeitpunkt geltend gemacht werden kann. Vorteil des Vorausvermächtnisses ist hier, dass der Begünstigte die Rechtsposition bereits vor Auseinandersetzung erhält, da der Vermächtnisanspruch als Nachlassverbindlichkeit bereits mit Eintritt des Erbfalls bzw. Eröffnung der letztwilligen Verfügung geltend gemacht werden kann.[60]

Im Rahmen eines Vermächtnisses besteht jedoch die Gefahr, dass die Erben (möglicherweise entgegen des Erblasserwillens) von den Dateninhalten Kenntnis erlangen. Das (Voraus-)Vermächtnis stellt zwar einen schuldrechtlichen Anspruch auf Übertragung der Rechtsposition dar. Vor Erfüllung des Vermächtnisses fällt der Vermächtnisgegenstand jedoch zunächst in den Nachlass, sodass vorheriger Zugriff und Einsichtnahme durch die Erben trotzdem möglich sind.[61] Um dies zu verhindern, ist

[56] *Ann*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2048 Rn. 9.
[57] *Müller-Christmann*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 1939 Rn. 2; *Hölscher*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 2150 Rn. 4, § 2147 Rn. 3.
[58] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 365.
[59] *Seidler*, Digitaler Nachlass, S. 152.
[60] So auch *Seidler*, Digitaler Nachlass, S. 152.
[61] *Gloser*, MittBayNot 2016, S. 101 (107); *Seidler*, Digitaler Nachlass, S. 152 f.

dem Erblasser anzuraten, Kontrollmechanismen (wie Auflagen oder Testamentsvollstreckung) in die letztwillige Verfügung zu integrieren.[62]

6.4.2.4 Vermächtnis

Wird der Begünstigte nicht zugleich als Erbe eingesetzt, können die Datenbestände auch mittels eines Vermächtnisses gemäß §§ 1939, 2147 BGB zugewendet werden. Erneut können nicht die Daten an sich vererbt werden, allerdings kann auch hier ein lokales Speichermedium mitsamt den darauf befindlichen Daten oder die Online-Vertragsbeziehungen hinsichtlich der auf fremden Servern gespeicherten Daten vermacht werden.[63]

Hinsichtlich der Vor- und Nachteile gilt entsprechend das soeben zum Vorausvermächtnis Angeführte mit dem Unterschied, dass der Vermächtnisnehmer nicht Erbe wird.

6.4.2.5 Auflage

Daneben ist denkbar, dass der Erblasser eine Auflage anordnet, die die Erbengemeinschaft verpflichtet, der begünstigten Person die Rechtsposition, also den digitalen Nachlassgegenstand, zu übertragen. Nachteil einer solchen Auflage ist jedoch, dass es nur einseitig die Erben verpflichtet, der Begünstigte selbst aber keinen Anspruch auf Erfüllung der Auflage hat.[64] Insofern kann sich die Durchsetzung des Anspruchs für den Begünstigten schwierig gestalten, wenn sich die Erben weigern, die Auflage zu erfüllen und den digitalen Nachlassgegenstand zu übertragen. Somit stellt sich das Vermächtnis für den Begünstigten als stärkere Rechtsposition dar, da in diesem Fall die Erfüllung auch gerichtlich durchgesetzt werden kann.

6.4.3 Befugnisse der Erben/Begünstigten

Nach der in Kapitel 2 auf Seite 35 beschriebenen gesetzlichen Ausgangslage hat der Erbe oder Vermächtnisnehmer des digitalen Nachlasses umfassende Einsichts- und Nutzungsrechte. Möchte der Erblasser jedoch erreichen, dass der Begünstigte im Fall seines Todes in einer bestimmten Weise mit dem digitalen Nachlass verfährt, kann er diesbezüglich Auflagen im Sinne der §§ 1940, 2191 ff. BGB anordnen.

Neben der Verhinderung des Zugriffs auf bestimmte Datenbestände (siehe Kapitel 6.4.1.1 auf Seite 182) ist es möglich, dass der Erblasser einen Erben mittels Auflage oder auch einen Testamentsvollstrecker verpflichtet, beispielsweise eine Homepage nach den Vorstellungen des Erblassers und unter Hinweis auf den Todesfall weiterzuführen. Hier besteht die Pflicht, unverzüglich das Impressum

[62] Dazu sogleich ausführlich.

[63] *Gloser*, MittBayNot 2016, S. 101 (107), ist hier insofern ungenau, als er davon spricht, die „Rechte an den Daten“ zu vermachen.

[64] *Seidler*, Digitaler Nachlass, S. 152.

zu ändern, vgl. § 6 TMG.[65] Dabei kann der Erblasser den insoweit Verpflichteten ein Ermessen hinsichtlich des Umgangs mit den Vertragsbeziehungen und Daten einräumen. Allerdings kann er auch genaue Vorgaben treffen, wie nach seinen Vorstellungen mit dem digitalen Nachlass zu verfahren ist. Dabei ist der Erblasser – in den Grenzen der Rechtsordnung – sehr frei. So kann beispielsweise für jede Vertragsbeziehung eine eigene Verhaltensanordnung getroffen werden, oder eine Verpflichtung, einen Online-Nachruf einzustellen. Auch kann ein Recht auf Einsicht gegeben werden, jedoch unter der Auflage, dass Nutzerkonten nicht aktiv weitergenutzt werden. Wie stets sollten die Anordnungen möglichst konkret getroffen werden, um (Rechts-)Unsicherheiten und Streitigkeiten zu vermeiden.[66]

Um diese Verfügungen weiter abzusichern, ist es möglich, dass diese Auflagen durch eine auflösende Bedingung der Erbeinsetzung i. S. d. §§ 158 II, 2075 BGB begleitet werden. Erfüllen die Erben eine Auflage nicht, die dauerhaft ein Tun oder Unterlassen von den Erben fordert, verlieren sie ihr Erbrecht. Zu beachten ist jedoch, dass es sich nur dann um eine echte auflösende Bedingung handelt, wenn nicht nur eine einmalige Handlung oder ein Tun oder Unterlassen über einen bestimmten Zeitraum betroffen ist.[67] Zudem kann eine solche auflösende Bedingung zwar abschreckend wirken. Allerdings setzt auch dies voraus, dass eine dritte Person (dies kann auch ein Miterbe sein) die Einhaltung der Auflage überprüft.

Daher ist eher zu empfehlen, zur Kontrolle der Auflagenerfüllung Testamentsvollstreckung anzuordnen und so eine Überwachung der Begünstigten zu erreichen.[68]

6.4.4 Kontrolle der Erben/Begünstigten

6.4.4.1 Testamentsvollstreckung

Möchte der Erblasser sicherstellen, dass seinen Verfügungen Folge geleistet wird oder möchte er einfach nur eine sachkundige Person mit der Verwaltung des Nachlasses betrauen, ist die Einsetzung eines Testamentsvollstreckers möglich, der entweder allein mit der „Verwaltung digitaler Daten“ oder des gesamten Nachlasses einschließlich des digitalen Nachlasses betraut ist.[69] Der Testamentsvollstrecker hat dann die Aufgabe, den Nachlass zu verwalten, § 2205 BGB, wobei der Erblasser ihm konkrete Anordnungen für die Art und Weise der Verwaltung erteilen kann, § 2216 BGB. Auch hier

[65] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 77.

[66] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 81 f., mit weiteren konkreten Beispielen.

[67] *Leipold*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2075 Rn. 4 ff.; Zu beachten ist jedoch, dass sich diesbezüglich Probleme hinsichtlich des Nachweises des Erbrechts ergeben können, dazu noch ausführlich in Kapitel 6.6.2 auf Seite 232.

[68] *Gloser*, MittBayNot 2016, S. 101 (107); *Raude*, RNotZ 2017, S. 17 (27); zur Überwachung der Begünstigten siehe das folgende Kapitel.

[69] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 77; *Deusch*, ZEV 2018, S. 687 (690); zu Problemen bei der Testamentsvollstreckung vgl. *Uhrenbacher*, ZEV 2018, S. 248 ff., die jedoch entgegen der Ansicht des *BGH* eine Zugriffsmöglichkeit sowohl der Erben als auch des Testamentsvollstreckers auf den digitalen Nachlass aufgrund des § 88 III 3 TKG verneint.

sollte eine Person ausgewählt werden, die den erforderlichen technischen Sachverstand hinsichtlich der Handhabung des digitalen Bereichs aufweist.[70]

Zwar ist eine Testamentsvollstreckung nicht allein deshalb notwendig, weil es sich um den digitalen Nachlass handelt.[71] Allerdings ist eine solche Anordnung aufgrund der Verschwiegenheit des Testamentsvollstreckers[72] insbesondere dann zu empfehlen, wenn es sich um private Daten handelt, nur bestimmte Erben Einsicht nehmen sollen oder der digitale Nachlass im Wege des Vermächtnisses einer Person zugedacht wurde. Ein Testamentsvollstrecker ist durch die ihm eingeräumte Vertretungs- und Verfügungsbefugnis berechtigt, (Voraus-)Vermächtnisse zu erfüllen oder Verträge mit Online-Dienstanbietern zu kündigen, falls dies in der letztwilligen Verfügung vorgesehen und möglicherweise sogar mit einer Auflage verbunden ist. Wie bereits beschrieben, besteht im Rahmen der Anordnung eines (Voraus-)Vermächtnisses die Gefahr, dass die Erben vor Erfüllung des Vermächtnisses auf die Daten zugreifen. Hier kann der Testamentsvollstrecker den Zugriff der Erben vor Erfüllung des Vermächtnisses verhindern.[73] Daneben kann dies auch dadurch verhindert werden, dass das (Voraus-)Vermächtnis mit einer Auflage verbunden wird, nach der den Erben untersagt ist, Einsicht in die Konten/Datenträger zu nehmen oder diese zu nutzen. Die Vollziehung dieser Auflage kann nach § 2194 S. 1 BGB verlangt werden.[74] Zu berücksichtigten ist allerdings, dass ein reiner Vermächtnisnehmer, der nicht zugleich Erbe ist, diese Vollziehung nicht verlangen kann.[75] Der Erblasser könnte jedoch nach herrschender Meinung den Vermächtnisnehmer als weitere vollziehungsberechtigte Person durch Verfügung von Todes wegen bestimmen.[76] Zudem könnte wohl auch der Vermächtnisnehmer selbst als Testamentsvollstrecker bestellt werden.[77]

Neben der möglichen Verwaltungsanordnung, dass der Testamentsvollstrecker Benutzerkonten oder auch Daten löschen soll,[78] kann er auch damit beauftragt werden, sämtliche Konten zu löschen und die dazugehörigen Daten zu sichern, um diese den vom Erblasser ausgewählten Personen zur Verfügung zu stellen.[79]

Da der Testamentsvollstrecker jedoch nur vertretbare Handlungen ausführen kann, ist ihm die Durchsetzung einer Unterlassungspflicht der Erben nur insoweit möglich, als er von den Erben (gegebenenfalls klageweise) gemäß §§ 2194 BGB i. V. m. 2208 II BGB die Vollziehung der Auflage, also beispielsweise die Unterlassung der Einsichtnahme, fordern kann.[80]

[70] *Steiner/Holzer*, ZEV 2015, S. 263 (266); *Schleifenbaum*, ErbR 2015, S. 230 (236).
[71] *Gloser*, MittBayNot 2016, S. 101 (104).
[72] *Schleifenbaum*, ErbR 2015, S. 230 (236).
[73] *Raude*, RNotZ 2017, S. 17 (26); *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 82.
[74] *Seidler*, Digitaler Nachlass, S. 152 f.
[75] *Burandt*, in: Burandt/Rojahn, Erbrecht, § 2194 Rn. 2 ff.
[76] *Rudy*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2194 Rn. 5; *Otte*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 2194 Rn. 6; *Seidler*, Digitaler Nachlass, S. 153.
[77] *Raude*, RNotZ 2017, S. 17 (27).
[78] *Gloser*, MittBayNot 2016, S. 101 (107); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 77.
[79] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 77.
[80] *Seidler*, Digitaler Nachlass, S. 154.

6.4.4.2 Vorsorgevollmacht im Vergleich zur Testamentsvollstreckung

Im Grundsatz kann eine diesbezügliche Kontrolle und Nachlassverwaltung auch durch einen Vorsorgebevollmächtigten mit trans- oder postmortaler Vollmacht durchgeführt werden.

Vorteil insbesondere der transmortalen Vorsorgevollmacht ist, dass der Bevollmächtigte unmittelbar mit Eintritt des Erbfalls tätig werden und den Zugriff der Erben verhindern kann. Ein Testamentsvollstrecker muss demgegenüber nach Eröffnung der Verfügung von Todes wegen zunächst in sein Amt berufen werden und dieses annehmen, § 2202 BGB. Davor ist der Testamentsvollstrecker nicht befugt, Handlungen für den Nachlass vorzunehmen. Auch der Erbe darf nicht tätig werden, da er gemäß § 2211 BGB aufgrund der Testamentsvollstreckung einer Verfügungssperre unterliegt, die unabhängig von der Annahme der Testamentsvollstreckung eintritt.[81]
Nachteil der Vorsorgevollmacht gegenüber der Ernennung eines Testamentsvollstreckers ist die Widerrufsmöglichkeit der Vollmacht. Die Erben könnten also den Bevollmächtigten aus seinem Amt entfernen und so die Durchsetzung des Erblasserwillens vereiteln. Die Ausgestaltung als unwiderrufliche Vollmacht ist nur in engen Grenzen möglich und verhindert den Widerruf auch nicht gänzlich.[82]

Vorteil der Testamentsvollstreckung ist demgegenüber, dass sie von den Erben nicht einfach widerrufen werden kann.[83] Auch hat der Bevollmächtigte keine so weitgehenden Befugnisse wie sie für den Testamentsvollstrecker in den §§ 2203 ff. BGB gesetzlich festgehalten sind. Hier spielt insbesondere eine Rolle, dass der Bevollmächtigte kein Recht hat, den Erben aus seiner Position zu verdrängen, da die Bevollmächtigung keine Verfügungsbeschränkung der Erben zur Folge hat.[84] Durch Vollmacht kann nicht erreicht werden, dass die rechtsgeschäftliche Handlungsfähigkeit des vertretenen Erben begrenzt oder dem Vertreter sogar ein Weisungsrecht zugewiesen wird.[85] Möchte der Erblasser also insbesondere bestimmte Personen von dem Zugriff auf digitale Nachlassgegenstände gänzlich ausschließen, ist die Testamentsvollstreckung besser geeignet.[86]

Aufgrund der Schwächen der Vorsorgevollmacht gegenüber der Testamentsvollstreckung ist letztere in der Regel das wirkungsmächtigere Instrument, um dem Willen des Erblassers zur Geltung zu verhelfen. Um die Zeit zwischen Erbfall und Ernennung des Testamentsvollstreckers abzusichern, erscheint es jedoch möglich und sinnvoll, für diese Zwischenzeit einen Vorsorgebevollmächtigten zu bestellen, der die dringenden Geschäfte erledigen kann. Dabei kann auch der spätere Testamentsvollstrecker zunächst als Vorsorgebevollmächtigter berufen werden.[87] Auch kann dem Testamentsvollstrecker in Ergänzung eine Vorsorgevollmacht erteilt werden, beispielsweise damit er entgegen § 2205 S. 3 BGB auch unentgeltlich über Nachlassgegenstände verfügen darf.[88]

[81] *Werner*, ZErb 2019, S. 137.
[82] Siehe dazu bereits oben ausführlich.
[83] *Seidler*, Digitaler Nachlass, S. 156.
[84] So auch *Werner*, ZErb 2019, S. 137 (141).
[85] *Zimmermann*, in: Säcker u. a. (Hrsg.), MükoBGB, Vorbemerkung zu §§ 2197 ff. Rn. 16.
[86] *Seidler*, Digitaler Nachlass, S. 157.
[87] Ähnlich auch *Seidler*, Digitaler Nachlass, S. 157.
[88] *Werner*, ZErb 2019, S. 137.

6.5 Verfahren zur Bereitstellung von Zugangsdaten und Nachweisen

Im Rahmen eines Testaments oder einer Vorsorgevollmacht können Erblasser zu Lebzeiten regeln, was zum digitalen Nachlass gehört, und wie und an welche Erben dieser Nachlass übergeben werden soll, siehe vorige Kapitel 6.2 bis 6.4 auf den Seiten 176–181. Das Testament oder die Vorsorgevollmacht stellen die materiell-rechtliche Ermächtigung dar, die erforderlich ist, damit der Begünstigte im Rechtsverkehr als Rechtsnachfolger oder Stellvertreter des Nutzers auftreten kann. Zur praktischen Umsetzung der Vorsorge ist es jedoch empfehlenswert, dass der Verbraucher den Erben bzw. Stellvertretern eine Auflistung der vorhandenen Daten und Vertragsverhältnisse mit den dazugehörigen Zugangsdaten zur Verfügung stellt. Die rechtliche Vorsorge kann hierbei sinnvoll durch technische Maßnahmen ergänzt werden, um in der Praxis die Zugangsdaten des Nutzers den Erben bzw. Stellvertretern zur Verfügung zu stellen. Die Berechtigung durch Vollmacht oder als Erbe kann jedoch nicht durch die Zurverfügungstellung der Zugangsdaten ersetzt werden.

Bis heute werden die meisten Nutzerkonten digitaler Dienste mit Login-Daten bestehend aus Benutzernamen und Passwort geschützt. Als Benutzernamen werden häufig E-Mail-Adressen verwendet, weil diese weltweit eindeutig sind und sich die Nutzer damit keine zusätzlichen Benutzernamen für ihre Konten merken müssen. Die Nutzer können ihre Login-Daten im Webbrowser speichern, sodass sie nicht bei jedem Login neu eingegeben werden müssen. Dies kann es zumindest den Erben leichter machen, die Konten des Erblassers zu übernehmen, falls der Erblasser nicht für die Übergabe vorgesorgt hat, aber seine Rechner und Mobilgeräte vererbt. Allerdings sind die Login-Daten in den gängigen Webbrowsern grundsätzlich nur unzulänglich geschützt. Das BSI empfiehlt daher, die Option „Passwörter speichern“ im Webbrowser zu deaktivieren.[89] In keinem Fall handelt es sich um eine praktikable Option, Zugriffsdaten an die Erben weiterzugeben.

Ohne Zurverfügungstellung von Zugangsdaten kann es im Sterbefall für die Erben schwierig werden herauszufinden, welche Nutzerkonten des Erblassers überhaupt vorhanden sind. Dies ist vor allem auch für den (Berufs-)Betreuer wichtig, der möglicherweise die betreute Person vor Übernahme der Betreuung gar nicht kennt, um sich einen Überblick zu verschaffen. Technische Dienstleistungen von Nachlassdiensten werden gerade in denjenigen Fällen in Anspruch genommen, in denen der Erblasser verstarb, ohne eine Vorsorge für den digitalen Nachlass getroffen zu haben. Aufschlussreich für die Ermittlung von existierenden Konten ist vor allem die Analyse der vom Erblasser versendeten Mails, der installierten Anwendungen und Apps auf dem Mobiltelefon mit evtl. vorhandenen Historien (z. B. Webbrowser-Historie). Dies setzt natürlich einen Zugriff auf das E-Mail-Konto bzw. auf die vom Erblasser genutzten Geräte voraus. Manche Nachlassdienste verfügen über so gute Kontakte zu den wichtigsten Online-Diensten, dass sie bei den Anbietern vorhandene Konten ermitteln oder sogar die Löschung von Konten veranlassen können, siehe Kapitel 6.5.5 auf Seite 205. Falls der Erblasser in sozialen Medien aktiv war, kann die Analyse einer einzelnen Profilseite über die ggf. vorhandenen Links und Einträge Erkenntnisse über weitere Konten liefern. Suchmaschinen können eine solche Suche automatisiert durchführen und es gibt Online-Dienste, die gezielt nach Information über Personen

[89] BSI: Machen Sie Ihren Browser sicher, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/SicherheitsCheck/sicherheitscheck_node.html.

suchen.[90]

Eine Zurverfügungstellung von Zugangsdaten ist insbesondere dann hilfreich, wenn der Erblasser pseudonyme oder anonyme Konten besitzt, die im Sterbefall selbst dann nicht auffindbar wären, wenn die Erben oder andere autorisierte Instanzen mit dem Namen des verstorbenen Erblassers bei den Anbietern anfragten. Die damit verbundenen digitalen Werte sind ohne Kenntnis der Zugangsdaten für die Erben verloren. Die einfachste technisch-organisatorische Maßnahme durch den Erblasser bestünde darin, die Zugriffsdaten zum digitalen Nachlass auf Papier zu schreiben und für die Erben sichtbar zu hinterlegen. Dies liegt häufig auch im Interesse der Erblasser noch zu Lebzeiten, um selbst den Überblick über möglicherweise selten genutzte Konten und Passwörter zu behalten.

In Kapitel 6.5.1 auf der nächsten Seite wird zunächst klargestellt, weshalb eine Auflistung von Zugangsdaten in einer letztwilligen Verfügung oder Vorsorgevollmacht selbst nicht erfolgen sollte. In den darauf folgenden Kapiteln 6.5.2 auf Seite 195 bis 6.5.9 auf Seite 220 werden Möglichkeiten vorgestellt, um wichtige Zugriffsdaten und Nachweise für die Übergabe im Sterbefall vorzubereiten. Wichtige praktische Kriterien für die möglichen Vorsorgelösungen sind:

- **Zuverlässigkeit**: Dies meint vor allem die Langlebigkeit der Lösung, d. h. dass sie auch dann noch funktioniert und dass ggf. der Lösungsanbieter noch existiert, wenn der Sterbefall des Erblassers erst nach vielen Jahren eintritt. Bezieht das Verfahren zudem auch die Online-Dienstanbieter mit ein, sodass im Sterbefall eine rechtmäßige Übergabe der Konten an die Erben mit Wissen der Anbieter stattfinden kann?

- **Sicherheit**: Dies meint, wie sehr die Lösung die Authentizität (Echtheit), Integrität, Vertraulichkeit und Verfügbarkeit der Informationen zum digitalen Nachlass gewährleisten kann. Werden die Daten verschlüsselt und gibt es die Möglichkeit einer weiteren Authentisierung zusätzlich zu Benutzername / Passwort?

- **Datenschutz**: Die Nutzungsbedingungen und Datenschutzrichtlinien des Lösungsanbieters sollten klar darlegen, dass die Nutzer die Rechte an den Daten behalten und die Daten ausschließlich für den vorgesehenen Zweck verarbeitet werden. Bleibt es dem Anbieter grundsätzlich verwehrt, auf die Daten und kryptografischen Schlüssel der Nutzer zuzugreifen? Funktioniert die Lösung auch lokal bei den Nutzern, ohne dass der Anbieter involviert ist?

- **Gebrauchstauglichkeit**: Dies meint die Benutzungsfreundlichkeit der Vorsorgelösung und deren unkomplizierte Abwicklung im Sterbefall. Ist es für die Erblasser leicht und kostengünstig, die Daten für den Sterbefall zu archivieren? Ist es für die Erben leicht, die Daten zu finden und sie erfolgreich nutzbar zu machen? Ermöglicht die Lösung, gleich zu Beginn andere Personen (Vertrauenspersonen, Erben) einzubeziehen bzw. mehrere Nutzer anzulegen, die untereinander Daten freigeben können?

- **Mehrwert**: Bietet die Lösung einen Mehrwert, beispielsweise dadurch, dass der Erblasser bereits zu Lebzeiten die Lösung nutzen kann und damit die Wahrscheinlichkeit erhöht, dass die Daten auch über viele Jahre aktuell gehalten werden?

[90] Beispielsweise listet die Seite https://jonamag.de/personensuche-im-netz-so-gehts solche Dienste auf.

Jede technische Maßnahme wird direkt nach ihrer Beschreibung rechtlich bewertet.

6.5.1 Auflistung der Zugangsdaten direkt in letztwilligen Verfügungen oder Vollmachten

Sowohl im Rahmen erbrechtlicher Verfügungen als auch von Vorsorgevollmachten sollten – um Streit hinsichtlich der wirksamen Erbberechtigung insbesondere mit ausländischen Dienstanbietern zu vermeiden – den Erben die Zugangsdaten zur Verfügung gestellt werden.

Abzuraten ist aber davon, sämtliche Zugangsdaten direkt in die Verfügung von Todes wegen oder eine Vorsorgevollmacht aufzunehmen. Zwar wäre so eine Kenntnisnahme durch die Begünstigten sichergestellt. Allerdings könnten auf diese Weise auch unberechtigte Personen von den Zugangsdaten in einer letztwilligen Verfügung erfahren. So könnten hinsichtlich des digitalen Nachlasses auch nicht begünstigte Erben oder Pflichtteilsberechtigte von den Zugangsdaten Kenntnis erlangen und sich unberechtigten Zugang zu den Nutzerkonten des Erblassers verschaffen.[91] Es besteht somit die Gefahr, dass die Zugangsdaten in falsche Hände geraten.[92] Ein noch größerer Personenkreis kann in den Inhalt einer Vorsorgevollmacht Einsicht nehmen, weil diese in der Regel dem jeweiligen Geschäftspartner (ggf. in Ausfertigung) zur Legitimation vorgelegt wird.[93] Somit könnte jeder Geschäftspartner des Vollmachtgebers und damit theoretisch eine unbeschränkte Zahl von Personen der Vollmacht die Zugangsdaten entnehmen.[94]

Zudem kann sich diese Vorgehensweise als sehr umständlich darstellen, da grundsätzlich empfohlen wird, Passwörter häufig zu ändern.[95] Nach jeder Änderung eines Passworts oder eines Nutzernamens, wenn neue Nutzerkonten eröffnet oder bereits bestehende gekündigt bzw. gelöscht werden, müsste – um das Ziel zu erreichen, den Zugriff der Erben zu erleichtern – auch die Urkunde geändert werden. Dies ist besonders aufwendig, wenn es sich um eine notarielle Vorsorgeurkunde, ein notarielles Testament oder ein Testament in amtlicher Verwahrung handelt, da in diesem Fall bei jeder Änderung die aufbewahrende Stelle aufgesucht werden müsste. Bei notariellen Urkunden kommt hinzu, dass die grundsätzlich empfohlene häufige Änderung der Passwörter auch zu unnötig hohen Notarkosten führen kann, da mit jeder Passwortänderung oder jedem neuen Abschluss einer Online-Vertragsbeziehung die Urkunde durch den Notar geändert werden müsste.[96]

[91] *Salomon*, NotBZ 2016, S. 324 (328 f.); ähnlich auch *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 74; *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[92] *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[93] *Salomon*, NotBZ 2016, S. 324 (329); *Herzog/Pruns*, Digitaler Nachlass, S. 160.
[94] *Raude*, RNotZ 2017, S. 17 (24 f.).
[95] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Digitaler Nachlass Rn. 97; *Kutscher*, Digitaler Nachlass, S. 150; *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ 2015, 4 (11 f.).
[96] *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 74.

6.5.2 Zugangsdaten mittels Passwort-Vergessen-Funktion

6.5.2.1 Technische Darstellung und Bewertung

Häufig hat der Erblasser zu Lebzeiten keinerlei Vorsorge getroffen, damit nach seinem Tod die digitalen Konten und Werte geregelt an die Erben übergeben werden können. Online-Dienste sehen meist die klassische Anmeldung mit Benutzername (oftmals die E-Mail-Adresse) und Passwort vor. Für den Fall, dass Benutzer ihr eigenes Passwort vergessen haben, dient die Funktion „Passwort vergessen". Für die Erben, die die Konten des Erblassers einsehen möchten, aber die Passwörter nicht kennen, ist es naheliegend, diese Funktion zu nutzen, um neue, ihnen bekannte Passwörter setzen zu können. Wird auf den entsprechenden Link geklickt, sendet der Dienstanbieter ein neues, temporär gültiges Passwort per E-Mail an die hinterlegte E-Mail-Adresse oder per SMS an die hinterlegte Handynummer. Die Erben benötigen also mindestens den Zugang zum E-Mail-Konto oder den Zugriff auf das Smartphone des Erblassers, je nachdem, welche Daten der Kontoinhaber für diesen Zweck bei den Diensten hinterlegt hatte.

Mitunter werden noch zusätzliche Sicherheitsfragen gestellt, deren Antworten der Kontoinhaber bei der Erstregistrierung hinterlegt hatte. Typische Sicherheitsfragen sind die Frage nach dem Namen des ersten Haustieres oder die Frage nach dem Mädchennamen der Mutter. Die hinterlegten Antworten können möglicherweise von den Erben recherchiert werden. Aber auch Angreifer können versuchen, über die Passwort-Vergessen-Funktion Zugang zu den hinterlegten E-Mail-Adressen zu bekommen, SMS abzufangen, die Antworten zu den Sicherheitsfragen zu recherchieren oder mittels „Social Engineering" den telefonischen Kundensupport des Anbieters dazu zu bringen, ein neues Passwort an eine alternative E-Mail-Adresse zu senden. Die Sicherheit solcher Funktionen wurde deshalb schon häufig infrage gestellt.[97,98]

Die Nutzung der Passwort-Vergessen-Funktion durch Erben erfolgt in der Regel nicht im Sinne der Anbieter, die nach wie vor den eigentlichen Kontoinhaber und nicht einen Erben hinter der Aktion vermuten. Haben die Erben nach dem Setzen neuer Passwörter Zugriff auf die Konten des Erblassers erhalten, können sie prinzipiell all die Nutzerdaten aktualisieren, die auch der Erblasser als rechtmäßiger Kontoinhaber aktualisieren durfte, beispielsweise Vor- und Nachnamen, postalische Adresse, E-Mail-Adresse und Bankverbindungsdaten. Damit werden die Konten faktisch von den Erben übernommen, ohne die betreffenden Online-Dienstanbieter explizit darüber zu informieren. Die Erben können sich nicht sicher sein, dass die Anbieter diesen Wechsel akzeptieren werden.

Fazit: Die existierenden Passwort-Vergessen-Funktionen bieten keine gute Vorsorgemöglichkeit für den digitalen Nachlass. Die Erben müssen Zugriff auf das im jeweiligen Dienst hinterlegte E-Mail-Konto und evtl. auch auf das Smartphone des Erblassers haben, um in einem Dienst ein neues Passwort setzen zu können.

[97] Golem.de (25.02.2019): Wie sich „Passwort zurücksetzen" missbrauchen lässt, https://www.golem.de/news/sicherheit-wie-sich-passwort-zuruecksetzen-missbrauchen-laesst-1902-139573.html.

[98] *Micklitz/Ortlieb/Staddon*, „I hereby leave my email to ...": data usage control and the digital estate, in: 2013 IEEE Security and Privacy Workshops, S. 42–44.

6.5.2.2 Rechtliche Bewertung

Die Nutzung der Passwort-Vergessen-Funktion ist auch aus rechtlicher Sicht keine geeignete Vorsorgemaßnahme, da jedenfalls die Zugangsmöglichkeit der Erben oder des Stellvertreters zu dem E-Mail-Konto des Verbrauchers erforderlich ist. Hat der Verbraucher keinerlei Zugangsdaten hinterlassen, müssten die Begünstigten somit gegenüber dem Dienstanbieter des E-Mail-Kontos einen Auskunftsanspruch geltend machen. Hierfür ist mindestens die Kenntnis erforderlich, welchen E-Mail-Dienst der Verbraucher verwendet hat. Auch sind die Begünstigten davon abhängig, dass der Dienstanbieter kooperiert.

Vorgeschlagen wurde daher, dass die Zugangsdaten zu einem E-Mail-Konto, über das andere Accounts verwaltet werden, an die Erben weitergegeben werden. Dieses könnte dann dazu verwendet werden, nicht vorhandene Passwörter zurückzusetzen. Das E-Mail-Konto sei insoweit „Dreh- und Angelpunkt“ der Internetaktivitäten. So müssten auch nicht alle Zugangsdaten an die Erben weitergegeben werden. Zumindest muss aber auch hier bekannt sein, welche Dienste der Erblasser genutzt hat.[99]

Diese Lösung ist zwar aus rechtlicher Sicht durchaus denkbar. Allerdings ist sie nur zielführend, wenn tatsächlich alle Online-Aktivitäten über diese eine E-Mail-Adresse verwaltet werden. Nutzt der Erblasser oder Vollmachtgeber mehrere E-Mail-Adressen parallel, müssten insoweit auch die Zugangsdaten für alle E-Mail-Adressen weitergegeben werden.

Auch ist diese Möglichkeit mit relativ hohem Aufwand für die Erben bzw. Bevollmächtigten verbunden. Zwar können sie zeitnah über das E-Mail-Konto verfügen. Um auf andere Nutzerkonten des Erblassers/Vollmachtgebers zugreifen zu können, müssen sie jedoch erst für jedes einzelne Nutzerkonto die Passwort-Vergessen-Funktion aktivieren. Dies stellt sich auch dann als schwieriger dar, wenn zusätzlich Sicherheitsfragen gestellt werden, auf welche die Begünstigten nicht sicher eine Antwort wissen. Insofern ist es nicht empfehlenswert, dass der Erblasser oder Vollmachtgeber die Passwort-Vergessen-Funktion als einzige Zugriffsmöglichkeit der Begünstigten vorsieht.

6.5.3 Zugangsdaten im Passwort-Manager

6.5.3.1 Technische Darstellung und Bewertung

Erblasser können für das digitale Erbe besser vorsorgen, wenn sie zu Lebzeiten die Übersicht und Kontrolle über vorhandene Accounts und Passwörter behalten. Passwort-Manager sind Programme in Form einer lokal installierten Software oder eines Online-Dienstes, die die vom Nutzer besuchten Internetseiten mit den dazugehörigen Benutzernamen und Passwörtern speichern und mit einem Masterpasswort schützen können. Anstelle von vielen verschiedenen Passwörtern muss nur noch das Masterpasswort gemerkt bzw. im Sterbefall an die Erben weitergegeben werden.

[99] *Herzog/Pruns*, Digitaler Nachlass, § 9 C Rn. 8 f.

Das BSI empfiehlt die Verwendung von Passwort-Manager-Programmen, insbesondere als Alternative zur weit verbreiteten unsicheren Praxis, dasselbe Passwort für mehrere Nutzerkonten zu benutzen.[100] Allerdings gibt es Untersuchungen darüber, dass durch Passwort-Manager viele Passwörter länger als nötig ungeschützt im Arbeitsspeicher des Rechners liegen und von Schadprogrammen ausgelesen werden könnten.[101] Eine höhere Sicherheit im Umgang mit Passwort-Managern wird mit einer Zwei-Faktor-Authentisierung erreicht, indem zusätzlich zur Eingabe des Masterpassworts ein einmaliger Code, z. B. eines separaten TAN-Generators oder einer empfangenen SMS, in den Passwort-Manager eingegeben werden muss. Eine Weitergabe an die Erben wird damit aber komplizierter, da zusätzliche Erklärungen und meist der Zugriff auf ein Gerät wie TAN-Generator oder Smartphone erforderlich werden.

Stellvertretend für die zahlreichen im Internet angebotenen Lösungen, die ihren Fokus auf die Verwaltung von Passwörtern legen, werden im Folgenden einige verbreitete Produkte vorgestellt, die im Kontext des digitalen Nachlasses interessant sein könnten.

- LastPass[102] des US-amerikanischen Anbieters LogMeIn ist ein Passwort-Manager in Form einer Webbrowser-Erweiterung und einer App für Mobilgeräte. Nach Herstellerangaben werden das Masterpasswort sowie die AES-Schlüssel zum Ver- und Entschlüsseln der Daten ausschließlich lokal auf dem Gerät verwendet. Die verschlüsselten Daten werden auf Cloud-Servern gespeichert. Eine Zwei-Faktor-Authentisierung wird unterstützt, z. B. die Eingabe eines zusätzlichen Time-Based One-Time-Password (TOTP)[103] der Authenticator-Software von LastPass oder eines anderen Anbieters oder die Präsentation eines USB-Tokens. Die Familien- und Premium-Varianten bietet „One-to-many sharing“ (Freigeben von Elementen in Ordnern) und „Emergency access“ (Zugriffsmöglichkeit für weitere Personen für den Notfall).

- PasswordBox[104] des spanischen Anbieters Softonic ist ein Passwort-Manager, der eine Datenbank in der Cloud nutzt und die Zugriffsdaten auf Webseiten Endgeräte-übergreifend in verschlüsselter Form bereitstellt. Dazu blendet PasswordBox die Zugangscodes automatisch ein, sobald man auf den betreffenden Webseiten surft. Auf Basis des Masterpassworts werden die einzelnen Zugangscodes lokal AES-verschlüsselt und an die Datenbank gesendet.

- 1Password[105] des gleichnamigen kanadischen Anbieters ist eine Online-Lösung, mit der Benutzer ihre Passwörter und Dokumente verwalten können. Dabei werden die Daten auf allen dazu freigegebenen Geräten synchronisiert. In der Familienversion kann der Zugriff auf Daten für Angehörige freigegeben werden. Nach Herstellerangaben wird für die lokale Verschlüsselung ein AES-256-Schlüssel vom Masterpasswort und einer individuellen 128-Bit-Kennung abgeleitet. Auch eine 2-Faktor-Authentisierung mit TOTP wird unterstützt.

[100] Siehe BSI, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.
[101] Siehe https://www.securityevaluators.com/casestudies/password-manager-hacking.
[102] LastPass: https://www.lastpass.com/de.
[103] TOTP ist ein Verfahren nach dem Internet-Standard RFC 6238
[104] PasswordBox: https://passwordbox.de.softonic.com.
[105] 1Password: https://1password.com/de.

- KeePass[106] ist ein kostenloser, quelloffener Passwort-Manager von Dominik Reichl (Deutschland). Die integrierte Passwortdatenbank wird mit einem Hauptschlüssel wahlweise mit AES, Twofish-Algorithmus oder ChaCha20 verschlüsselt. Zusätzlich zum Masterpassword kann, beispielsweise von einem USB-Stick, eine Schlüsseldatei eingelesen und zur Ableitung des Hauptschlüssels verwendet werden. Die Passwörter können zwischen verschiedenen Geräten synchronisiert werden, wenn die Datenbank entsprechend zugänglich abgelegt wird. Erweiterte Versionen bieten zusätzlich die Möglichkeit, dass sich die Benutzer mittels Challenge-Response mit einem Schlüssel auf einem nicht-auslesbaren Yubikey (ein USB-Sicherheitstoken) einloggen. Der Nutzer kann sich auch mit einem Schlüssel seines Windowskontos bei KeePass anmelden. KeePass stellt die gespeicherten Passwörter auf verschiedene Weise bereit: Über die manuelle Kopie in der Zwischenablage, mit dem Tastenkürzel $Strg + Alt + A$ oder automatisch direkt über KeePass in die Anwendungen. Dafür gibt es auch entsprechende Webbrowser-Plugins. Die Verwendung der Datenbank durch mehrere Nutzer ist nicht explizit vorgesehen. Es wird aber in jedem Fall das Ausdrucken eines sogenannten Notfallblatts empfohlen. Dieses enthält alle wichtigen Informationen, die zum Öffnen der Datenbank erforderlich sind.

Die Tabelle 6.1 zeigt einige Eigenschaften der Passwort-Manager im Überblick. Die in der Kopfzeile genannten Eigenschaften bedeuten Folgendes: „Offline-Lsg“ steht für die Eigenschaft, dass der Passwort-Manager auch ausschließlich lokal und offline beim Nutzer konfiguriert und verwendet kann. Dies kann als die sicherste Variante gelten, insofern der Anbieter keinen Zugriff auf Schlüssel und Daten des Nutzers erhält. „Local Encrypt“ bedeutet, dass die Nutzerdaten mit lokalen Schlüsseln verschlüsselt werden, dann aber in der Regel zum Anbieter übertragen werden. „2-Factor-Auth“ steht für die Möglichkeit, dass die Nutzer eine 2-Faktor-Authentisierung (z. B. Präsentation eines Hardware-Token zusätzlich zum Passwort) einsetzen und damit für mehr Sicherheit sorgen können. „Sharing“ steht für die Option, Passwörter für mehrere Nutzer anzulegen und die eigenen Daten für andere Nutzer freizugeben, was für die Übergabe eines digitalen Nachlasses nützlich sein kann.

Produkt	Offline-Lsg	Local Encrypt	2-Factor-Auth	Sharing
LastPass	—	✓	✓	✓
PasswordBox	—	✓	—	—
1Password	—	✓	✓	✓
KeePass	✓	✓	✓	—

Tabelle 6.1: Eigenschaften von Passwort-Managern

Fazit: Passwort-Manager können den Erbenden den Zugang zu den Accounts des Erblassers erleichtern, da der Erblasser den Erben prinzipiell nur das Masterpasswort übermitteln muss. Wenn der Passwort-Manager nicht direkt zum Einloggen in die Dienste verwendet werden kann, muss der Erblasser aber zu Lebzeiten die Disziplin aufbringen, nach jeder Passwortänderung an einem Online-Dienst manuell auch den entsprechenden Eintrag im Passwort-Manager zu aktualisieren. Ansonsten

[106] KeePass: https://keepass.info.

wären im Todesfall die gespeicherten Login-Daten für die Erben teilweise unbrauchbar. Die vorgestellten Passwort-Manager übertragen in der Regel lokal verschlüsselte Daten online auf die Server des Lösungsanbieters. Dies ermöglicht Gebrauchstauglichkeit, weil die Synchronisation und Nutzung der Daten auf verschiedenen Geräten keine besonderen Aktionen der Nutzer voraussetzt. Die Nutzer müssen allerdings dem Anbieter vertrauen, dass die Daten tatsächlich nicht auf dem Server entschlüsselt werden können, auch dann nicht, wenn staatliche Stellen oder Geheimdienste von den Anbietern den Zugang zu den Daten forderten. Ein Nachweis dieser wichtigen Sicherheitseigenschaft gegenüber den Nutzern ist kaum möglich. In dieser Hinsicht hat die KeePass-Lösung ein Alleinstellungsmerkmal, da Nutzer den Quellcode der Software auf missbräuchliche „Hintertüren“ überprüfen können und die Lösung unabhängig von einem Anbieter funktioniert. KeePass bietet viele zusätzliche Sicherheitsoptionen, die allerdings nur begrenzt laientauglich sind.

Grundsätzlich bezieht keines der Produkte die eigentlichen Online-Dienstanbieter mit ein, für deren Dienste die Nutzer die Zugriffsdaten im Password-Manager sichern. Im Sterbefall werden bestenfalls die Zugriffsdaten an die Erben übergeben, eine echte Übergabe mit Kenntnisnahme aufseiten der Online-Dienstanbieter findet jedoch nicht statt. Eine denkbare Verbesserung von Passwort-Managern im Sinne des digitalen Nachlasses wäre zumindest die automatische Mitteilung des Masterpassworts an Vertrauenspersonen im Notfall bzw. Sterbefall des Nutzers. In Kapitel 6.5.4 auf der nächsten Seite werden Dienste vorgestellt, die es ermöglichen, Daten für Vertrauenspersonen zu hinterlegen und automatisch freizugeben.

6.5.3.2 Rechtliche Bewertung

In der juristischen Literatur werden Passwort-Manager teilweise als möglicher Weg beschrieben, Zugangsdaten an die Erben weiterzugeben, statt diese beispielsweise auf Papier oder einem USB-Stick zu speichern.[107]

Allerdings wird insoweit nicht unterschieden, ob es sich bei dem Passwort-Manager um eine Online- oder Offline-Lösung handelt. Gegen die Nutzung von kommerziellen Dienstanbietern, die Online-Lösungen anbieten, bestehen generelle rechtliche und praktische Bedenken,[108] sodass deren Nutzung nicht empfohlen werden kann.

Denkbar ist jedoch eine Verschlüsselung der Zugangsdaten mittels der Offline-Lösung von KeePass.[109] Die gegen Online-Lösungen vorzubringenden Einwände greifen hinsichtlich dieses Passwort-Managers nicht. Im Rahmen von KeePass befinden sich die Zugangsdaten nicht auf dem Server des Anbieters, sondern auf dem PC oder einem sonstigen lokalen Datenträger des Nutzers, sodass nicht dieselben Sicherheitsbedenken bestehen. Zudem ist die Nutzung von KeePass von der Langlebigkeit des Anbieters unabhängig. Hinsichtlich der Speicherung auf dem PC wird jedoch vor dem Zugriff durch Spähprogramme gewarnt, soweit der PC selbst mit dem Internet verbunden ist.[110]

[107] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 19; *Pruns*, ErbR 2018, S. 614 (621).

[108] Siehe hierzu ausführlich Kapitel 6.5.6 auf Seite 209

[109] *Gloser*, DNotZ 2015, S. 4 (13); *ders.*, MittBayNot 2016, S. 101 (106); *Bleich*, c't 2/2013, S. 62 (64); *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 14.

[110] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 13.

Auch ist für den Vorsorgefall darauf zu achten, dass bei dieser Offline-Lösung den Begünstigten genau der Datenträger zugänglich zu machen ist, auf dem das Programm abgespeichert ist. Sollen verschiedenen Personen verschiedene Zugangsdaten zugänglich gemacht werden, müssen auch mehrere Zugänge für KeePass dadurch geschaffen werden, dass verschiedene Speichermedien für das Programm geschaffen werden. Die Lösung erfordert von den Verbrauchern insofern eine gewisse Disziplin, als die Zugangsdaten in dem Passwort-Manager per Hand aktuell gehalten werden müssen, da keine automatische Konfiguration mit einem Server erfolgt. Zudem ist ein gewisses technisches Geschick erforderlich.

Hinsichtlich der Verwaltung des Notfallblatts und des Masterpassworts folgen in Kapitel 6.5.8 auf Seite 217 weitere Ausführungen.

6.5.4 Zugangsdaten in digitalen Datensafes

6.5.4.1 Technische Darstellung und Bewertung

Über die reinen Passwort-Manager hinaus gibt es Programme und Dienste, die jegliche Art von Dateien, z. B. wichtige Dokumente, Audio-, Bild- und Video-Dateien, archivieren und zur Weitergabe an andere Nutzer freischalten können. Ein solcher elektronischer Datensafe entspricht den herkömmlichen physischen Ordnern, Kartons, Stahlkassetten, in denen Nutzer wertvolle Dinge speichern. Der elektronische Safe hat u. a. den Vorteil, dass Informationen ohne Medienbruch gespeichert, aktualisiert, wiederverwendet und weitergegeben werden können. Einige Dienste bieten Hilfen für die Planung des digitalen Nachlasses an,[111] darunter die folgenden drei grundlegenden Funktionen, die der Erblasser zu Lebzeiten nutzen kann:[112]

- Hinterlegen von Zugriffsdaten für genutzte Online-Dienste (Passwort-Manager).
- Hinterlegen von Anweisungen, was im Sterbefall mit den Online-Konten geschehen soll.
- Hinterlegen von Kontaktdaten der Vertrauenspersonen, die den Sterbefall melden, die Zugriffsdaten empfangen und die Anweisungen ausführen sollen.

Der kostenpflichtige Online-Dienst Deathswitch führte 2006 sogenannte „DeathSwitches“ ein, d. h. das automatische Versendung von Nachrichten, wenn sich der Kontoinhaber eine gewisse Zeit nicht beim Dienst eingeloggt hatte.[113] Der Dienst ermöglichte es Nutzern, bis zu 30 verschlüsselte E-Mails mit Anhängen zu speichern, die zum Zeitpunkt ihres Todes versendet werden sollten. Dies wurde durch die Eingabe eines Passworts in vorgegebenen Zeitabständen durch den Benutzer bestimmt.

[111] Die private israelischen Webseite Digital Dust, https://digital-era-death-eng.blogspot.com/2012/07/before-death-managing-your-digital.html, hat eine Liste solcher Dienste veröffentlicht, die im Kontext des digitalen Nachlasses stehen. Auch die Webseite Digital Beyond, https://www.thedigitalbeyond.com/online-services-list bietet eine Liste entsprechender Online-Dienste, einschließlich digitaler Immobiliendienstleistungen, posthumer E-Mail-Services und Online-Gedenkstätten.

[112] *Brucker-Kley u. a.*, Passing and passing on in the digital world – Issues and solutions for the digital estate, in: IADIS 2013, S. 48–256.

[113] *Eagleman*, A brief history of death switches, in: Nature 443, 882.

Wurde das Passwort nach mehreren Aufforderungen nicht eingegeben, wurden die E-Mails an die angegebenen E-Mail-Empfänger versendet. Der Dienst wurde Ende 2015 vermutlich aufgrund mangelnder Nachfrage wieder eingestellt. Ähnliche DeathSwitches kommen aber heute in unterschiedlichen Diensten zur Anwendung.

Im Folgenden sind Beispiele von Online-Safes aufgeführt, die ihren Fokus auf die Benachrichtigung von Vertrauenspersonen und die Weitergabe von Dokumenten für den Notfall bzw. Sterbefall legen. Manche dieser Online-Safes haben einen DeathSwitch integriert, um eine automatische Übergabe der hinterlegten Dokumente an die Vertrauenspersonen einzuleiten. Die Dienste sind in der Regel kostenpflichtig oder werden im Rahmen eines anderen Vertrags (z. B. Bankkonto) den Kunden zur Verfügung gestellt.

- SecureSafe[114] der Schweizer DSwiss AG ist ein Online-Dienst zum Verwalten von Passwörtern und Dokumenten. Der Kontoinhaber kann individuelle Daten als Nachlass bestimmten Personen zuweisen. Mit Aktivierung der Datenvererbung wird ein mehrstufiger Prozess zur Weitergabe von Informationen ermöglicht. Der Prozess wird mit Eingabe eines Aktivierungscodes (von pdf oder Papierausdruck) durch die Vertrauensperson gestartet. Während der darauf folgenden Sperrfrist sendet SecureSafe E-Mails und SMS an den Kontoinhaber, der den Weitergabeprozess noch abbrechen kann. Nach Ablauf der Sperrfrist erhalten alle Begünstigten eine E-Mail/SMS mit der Nachricht, dass ihnen digitales Eigentum vererbt wurde. Die Login-Daten werden separat per SMS versendet. Das Original-Konto wird zum Zeitpunkt des Logins blockiert und nach wenigen Tagen gelöscht. Dabei werden alle Daten gelöscht, welche keiner Person zugewiesen wurden.

- Next of Kin[115] und Digital Deads Man Switch[116] sind opensource WordPress Plugins. Diese haben den Zweck, die vorhandenen WordPress-Seiten auch über den Tod der jeweiligen Seiteninhabers zu erhalten, indem sie die Aktivitäten des Inhabers im Wordpress-System überwachen. Die Plugins senden nach konfigurierbaren Zeitintervallen, in denen der Inhaber nicht aktiv war, mehrere Warn-E-Mails an den Inhaber und ggf. an eine weitere Person. Wenn der Inhaber auch dann nicht seinen Blog besucht und das Zeitintervall zurücksetzt, versendet das Plugin eine vorbereitete E-Mail an die dafür vorgesehenen Empfänger. Die Plugins dienen auch als Online-Gedenkstätte und ermöglichen – beispielsweise durch das Versenden der Passwörter für Blog, Domain, Webhost und E-Mail – die Verwaltung des Blogs durch eine andere Person.

- EverPlans[117] des US-amerikanischen Anbieters Beyondly ist ein Online-Dienst zur Organisation von Passwörtern, Dokumenten und Archiven, die mit anderen geteilt werden können. Die Daten werden wie üblich mit SSL transportgesichert und mit AES verschlüsselt abgelegt. Nach Aktivierung des zweistufigen Logins bekommt der Nutzer einen zusätzlichen Eingabecode per SMS zugesendet, wenn nach Eingabe des letzten eindeutigen Codes mehr als 30 Tage vergangen sind oder die Anmeldung von einem nicht erkannten Gerät erfolgt. Zur Freischaltung

[114] SecureSafe: https://www.securesafe.com/de.
[115] Next of Kin: https://wordpress.org/plugins/next-of-kin.
[116] Digital Deads Man Switch: https://wordpress.org/plugins/wp-digital-dead-man-switch.
[117] EverPlans: https://www.everplans.com.

von Inhalten im Todesfall muss ein Stellvertreter den Todesfall an den Anbieter melden, der dann ein konfiguriertes Zeitintervall lang versucht, den Nutzer per E-Mail zu kontaktieren, mit der Möglichkeit, den Freischaltungsprozess abzubrechen.

- PartingWishes[118] des kanadischen Anbieters PartingWishes (mit weiteren Niederlassungen in den USA und in UK) bietet Mitgliedern an, US-amerikanische, kanadische und internationale Rechtsdokumente wie Testamente, Vollmachten, Patientenverfügungen, Nachlassanweisungen und Nachrichten, die nach ihrem Tod versendet werden sollen, auf Servern verschlüsselt zu speichern. Der Anbieter wirbt damit, dass die Nutzer auf diese Weise Anwaltskosten sparen können. Jeder Kontoinhaber kann weitere Schlüsselinhaber bestimmen. Diese erhalten eine ID (auf Wunsch auch vorab in Form eines Plastikausweises) für den Zugriff auf die Dokumente und können die Einsicht in die Dokumente anfordern. Dazu wird eine automatische Benachrichtigung an den Kontoinhaber gesendet. Reagiert der Kontoinhaber nicht innerhalb der von ihm selbst festgelegten Frist, werden die Dokumente an den Schlüsselinhaber freigegeben.

- E-Z-Safe[119] des israelischen Anbieters EasySafe ist ein Online-Safe für digitale Inhalte wie Finanz-, E-Mail- und Social-Network-Konten, Passwörter, Fotos, Videos, Aufzeichnungen und juristische Dokumente. Die Benutzer können aus verschiedenen Optionen wählen, wie die Inhalte bestimmten Personen zugänglich gemacht werden, und können das Benachrichtigungssystem beispielsweise so konfigurieren, dass zusätzlich eine Vertrauensperson die Inhalte freischalten muss.

- Docsafe[120] ist ein Online-Safe des Schweizer Telekommunikationsunternehmens Swisscom. Es soll vor allem dazu dienen, von verschiedenen Geräten aus auf wichtige Dokumente (z. B. Kopien von Pass und Flugtickets, Fotos) zugreifen und diese weiterleiten zu können. Zusätzlich zu Accountname und Passwort können weitere Authentisierungsverfahren eingestellt werden: Die Eingabe eines SMS-versendeten Zugangscodes oder die Identitätsprüfung mittels PIN-geschützter Mobile ID auf der SIM-Karte des Smartphones. Allerdings ist der Dienst auf Personen mit Schweizer Adresse und Schweizer Handynummer begrenzt.

- MyOnlineSafe[121] wird vom gleichnamigen Unternehmen betrieben und soll vor allem dem Zugriff auf Versicherungsdaten, Gesundheitsdaten und andere wichtige Dokumente dienen. Die Dokumente werden mit der Eingabe von Namen und E-Mail-Adressen der Vertrauenspersonen individuell schon zu Lebzeiten des Kontoinhabers freigegeben.

- Elektronischer Safe[122] ist ein Dienst, den die Sparkassen in Deutschland seit März 2018 ihren Kunden im Rahmen des Onlinebankings und des elektronischen Postfachs anbieten. Der Dienst soll der Langzeitablage von Kontoauszügen und anderen persönlichen Dokumenten dienen und wird mit Dokumentensicherheit „für die Ewigkeit“ beworben. Den Kunden stehen Speichergrößen zwischen 1 und 5 GB ohne Zusatzkosten zur Verfügung. Der Zugriff auf die Dokumente

[118] PartingWishes: https://www.partingwishes.com.
[119] E-Z-Safe: https://www.e-z-safe.com/Index.aspx.
[120] Docsafe: https://www.swisscom.ch/de/privatkunden/sicherheit/docsafe.html.
[121] MyOnlineSafe: https://www.myonlinesafe.com.
[122] Elektronischer Safe: https://www.f-i.de/News/ITmagazin/Archiv/2018/Sicher-ist-sicher-Langfristige-Kundenbindung-mit-dem-Elektronischen-Safe/Titelthema/Sicher-ist-sicher.

erfolgt defaultmäßig mit der zusätzlichen Eingabe einer TAN. Eine Freigabe der Dokumente an Vertrauenspersonen ist nicht explizit vorgesehen, würde aber im Todesfall des Kontoinhabers vermutlich zusammen mit dem Bankkonto abgewickelt werden. Betrieben wird der Dienst von der Finanz Informatik (FI), dem IT-Dienstleister der Sparkassen. Die Deutsche Bank bietet ihren Privatkunden mit eSafe[123] einen ähnlichen Service zur Ablage von digitalen Bankdokumenten, persönlichen Unterlagen und Passwörtern.

Die Tabelle 6.2 zeigt einige Eigenschaften der oben genannten Online-Safes im Überblick. Die in der Kopfzeile aufgeführten Eigenschaften bedeuten Folgendes: „Pwd-Mng“ steht für die zusätzliche Funktionalität eines Passwort-Managers. „DeathSwitch“ bedeutet, dass es einen Mechanismus gibt, um Vertrauenspersonen automatisch zu benachrichtigen, siehe Kapitel 7.4.1.1 auf Seite 318. „2-Factor-Auth“ steht für die Möglichkeit, dass die Nutzer eine 2-Faktor-Authentisierung (z. B. Präsentation eines Hardware-Tokens zusätzlich zum Passwort) einsetzen und damit für mehr Sicherheit sorgen können. „Sharing“ steht für die Option, die eigenen Daten für andere Nutzer freizugeben, „Memorial“ für die Möglichkeit, den Dienst als Online-Gedenkstätte zu nutzen. Die Spalte „Location“ gibt das Land an, in dem der Serverstandort des Dienstes vermutet wird.

Produkt	Pwd-Mng	DeathSwitch	2-Factor-Auth	Sharing	Memorial	Location
SecureSafe	✓	✓	✓	✓	—	CH
Next of Kin	—	✓	—	✓	✓	US
EverPlans	—	✓	—	✓	—	US
PartingWishes	—	✓	—	✓	✓	US
E-Z-Safe	—	✓	—	✓	—	IL
Docsafe	—	—	✓	✓	—	CH
MyOnlineSafe	—	—	—	✓	—	UK
Elektr. Safe	—	—	✓	—	—	DE

Tabelle 6.2: Eigenschaften von Online-Safes

Fazit: Die genannten kostenpflichtigen Dienste bieten meist ausreichend die Möglichkeit, die Weitergabe von wichtige Daten an Vertrauenspersonen vorzubereiten. Die Daten liegen allerdings auf den Servern der Lösungsanbieter, d. h. die Nutzer müssen den Anbietern vertrauen, dass diese nicht unbefugt auf die Daten zugreifen. Die meisten Anbieter haben ihren Sitz außerhalb der EU.[124] In jedem Fall müssen die Nutzer das Vertrauen besitzen, dass der Dienst über Jahrzehnte bestehen bleibt und nicht vorzeitig eingestellt wird. Daher ist die Tendenz verständlich, dass Banken in Deutschland für ihre Kunden einen solchen Dienst anbieten. In der Regel liegt aber der Fokus nicht auf der Vor-

[123] eSafe: https://www.deutsche-bank.de/pk/digital-banking/digitale-services/esafe.html.

[124] Auch bei Anbietern mit Sitz außerhalb der EU gilt das Marktortprinzip gemäß Art. 3 II DSGVO, wonach die Dienste, die datenschutzrechtlich relevante Geschäftsaktivitäten umfassen, ohne Rücksicht auf physische Organisations- oder Betriebsstrukturen der Unternehmen in den Anwendungsbereich der DSGVO fallen, siehe https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_7_Marktortprinzip.pdf

sorge des digitalen Nachlasses, sondern auf der Nutzung als sicherer Online-Speicher für wichtige Dokumente zu Lebzeiten.

Bietet ein Dienst eine DeathSwitch-Funktion, so erfolgen die Benachrichtigungen an die Kontoinhaber und Vertrauenspersonen in der Regel automatisch per E-Mail und SMS. Die Zeitintervalle und weiteren Bedingungen zur Auslösung der Weitergabe wird von den Kontoinhabern selbst konfiguriert. Dienste überprüfen vor der Freischaltung von Dokumenten an Vertrauenspersonen in der Regel keine amtlichen Nachweise (z. B. Sterbeurkunden), da es gar nicht im Interesse der Lösungsanbieter liegt, zu überprüfen, ob eine Übergabe der Zugriffsdaten und das Vererben der Online-Dienstkonten überhaupt rechtmäßig sind. Es gibt grundsätzlich keine Verknüpfung mit den vom Erblasser genutzten Online-Diensten wie soziale Netzwerke, Onlinebanking etc., sodass der Erblasser grundsätzlich für jeden genutzten Dienst separat Vorsorge treffen muss.

Soziotechnologische Untersuchungen zeigen zudem, dass die Nutzergewohnheiten, Informationen und Dokumente zu teilen, grundsätzlich ein besonderes Design von elektronischen Datensafes erfordern, dieses aber kaum gegeben ist. So sei es ungeachtet von Datensafes bei der Verwaltung digitaler Dokumente und Konten normale Praxis, Passwörter und Konten gemeinsam zu nutzen, Dokumente nicht strikt nach Personen zu ordnen und Dokumente im Auftrag von anderen Personen (z. B. innerhalb der Familie oder zwischen Partnern) zu verwalten. Nutzer würden häufig vernachlässigen, Anweisungen und weitergehende Informationen zu den Konten mitzuteilen, insbesondere was mit den Konten im Sterbefall geschehen soll, welche Informationen dahinter besonders wichtig sind oder gelöscht werden können. Die „wohlwollende Nachlässigkeit“, ohne Priorisierung möglichst alles zu speichern und die Sichtung den Nachkommen zu hinterlassen, sei teilweise emotional und stressbedingt, um mit der Fülle an Informationen und dem schwierigen Thema Vergänglichkeit zurechtzukommen. Elektronische Datensafes sollten dieses Nutzerverhalten berücksichtigen, indem sie beispielsweise die wechselnde Nutzung durch verschiedene Personen und Gruppen, das Verwalten im Auftrag und das Hinzufügen von Anweisungen und Prioritäten unterstützen.[125] Andere Forschungsgruppen entwerfen teilweise skurrile Geräte wie autonome Backup-Boxen und digitale Viewer zum automatischen Kopieren von Social-Media-Inhalten und zur Archivierung von Dokumenten.[126]

6.5.4.2 Rechtliche Bewertung

Neben der allgemein vorzubringenden Kritik an kommerziellen Dienstanbietern – siehe hierzu Kapitel 6.5.6 auf Seite 209 – ist vor allem hinsichtlich der DeathSwitch-Funktion bedenklich, dass die Daten ohne tatsächliche Überprüfung des Vorsorgefalls oder rechtliche Prüfung der materiell-rechtlichen Berechtigung weitergegeben werden. Insofern droht eine Gefahr des Missbrauchs, vor allem dann, wenn der DeathSwitch allein aufgrund der Benachrichtigung einer Vertrauensperson (wie bei SecureSafe) ausgelöst wird. Jedoch kann auch der Ablauf eines Zeitintervalls (wie bei Next of Kin oder

[125] *Pfister*, „This will cause a lot of work.“: Coping with transferring files and passwords as part of a personal digital legacy, in: CSCW '17, S. 1123–1138.

[126] *Odom u. a.*, Technology heirlooms? – Considerations for passing down and inheriting digital materials, in: CHI '12, S. 337–346.

Digital Deads Man Switch) den Vorsorgefall und vor allem die Rechtsnachfolge nicht mit der erforderlichen rechtlichen Sicherheit nachweisen.

Auch ohne Missbrauch droht die Herausgabe an Nichtberechtigte und die Umgehung erbrechtlicher Vorschriften. Zwar ist es grundsätzlich möglich, vertraglich die Übergabe von Nutzerkonten zu vereinbaren. Allerdings ist dies nur mit dem tatsächlichen Vertragspartner der Online-Vertragsbeziehung – also dem jeweiligen Betreiber der Plattform – möglich, nicht mit einer hinsichtlich des Vertrages dritten Person wie dem digitalen Datensafe, die keine Verbindung zu der Online-Vertragsbeziehung zwischen Nutzer und Dienstanbieter aufweist. Für eine wirksame Übertragung der Online-Vertragsbeziehung müsste der Nutzer somit eine vertragliche Vereinbarung mit dem Dienstanbieter der jeweiligen Plattform abschließen. Auch eine letztwillige Verfügung können die Datensafes nicht ersetzen, da diesbezüglich strenge Formvorschriften einzuhalten sind. Die tatsächliche Weitergabe der Zugangsdaten durch den digitalen Datensafe könnte insofern lediglich die Ermöglichung der faktischen Übergabe, aber keine materiell-rechtliche Berechtigung darstellen. Hinsichtlich der materiell-rechtlichen Vorsorge stellen die digitalen Datensafes daher keine Erleichterung dar, da der Erblasser neben der Nutzung des digitalen Datensafes mangels Verknüpfung desselben mit der jeweiligen Vertragsbeziehung für jedes von ihm genutzte Netzwerk noch gesondert Vorsorge treffen muss.

Soweit hinsichtlich der Herausgabe der Zugangsdaten ein bestimmtes Zeitintervall ablaufen muss, ist auch zu beachten, dass damit nicht auf dringende oder akut regelungsbedürftige Fälle reagiert werden kann.[127]

Auch die rechtliche Erleichterung hinsichtlich der Abspeicherung von Rechtsdokumenten bei einem Dienst wie PartingWishes ist fraglich. Jedenfalls ersetzt aus deutscher Sicht dieses digital gespeicherte Dokument nicht die Originalurkunde. Zum Beweis der Erbberechtigung oder der Bevollmächtigung ist im Rechtsverkehr aber immer noch regelmäßig die Originalurkunde oder mindestens eine beglaubigte Abschrift bzw. Ausfertigung derselben erforderlich. Ob dritte Personen – insbesondere die Dienstanbieter – die digital gespeicherten Dokumente als Nachweis ausreichen lassen, hängt wohl vom Einzelfall ab.

6.5.5 Zugangsdaten über digitale Nachlassdienste

6.5.5.1 Technische Darstellung und Bewertung

Privatwirtschaftliche Nachlassdienste bieten meist keine digitalen Datensafes an, sondern folgen in erster Linie dem Geschäftsmodell, die noch existierenden Vertragsbeziehungen von verstorbenen Erblassern zu ermitteln. Damit wird den Angehörigen und Bestattern gerade in dem sehr häufigen Fall geholfen, dass die Erblasser zu Lebzeiten keine Vorsorge für den digitalen Nachlass getroffen haben. Einige Dienste sehen zusätzlich vor, dass der Erblasser zu Lebzeiten dem Anbieter seine Konten und die damit verbundene Nachlassplanung mitteilt, d. h. dem Anbieter sagt, was im Sterbefall mit den

[127] Zu Googles Kontoinaktivität-Manager, wo sich jedoch ein vergleichbares Problem stellt: *Gloser*, MittBayNot 2016, S. 101 (105).

Konten geschehen soll. Digitale Nachlassdienste sind in der Regel Start-up-Unternehmen, und viele verschwinden nach einigen Jahren wieder vom Markt. Um eine sicherere wirtschaftliche Grundlage zu bekommen, versuchen einige Anbieter direkt mit Versicherungsgesellschaften, Behörden, Anwaltskanzleien und der Bestattungsbranche zusammenzuarbeiten, aber auch das gelingt nicht immer auf Dauer.[128] Manche Nachlassdienste kooperieren direkt mit den Online-Dienstanbietern, sodass die Nutzer beim Nachlassdienst keine Zugriffsdaten für den Zugriff auf ihre Online-Konten hinterlegen müssen.

Ein Beispiel ist der schwedische digitale Vererbungsdienst MyWebwill, der seine Dienstleistung ab 2010 anbot, allerdings bereits 2011 wieder einstellte.[129] Für 20 Euro pro Jahr nahm MyWebwill die Wünsche seiner Kunden für den Todesfall auf: „Du legst ein Konto an und teilst uns mit, bei welchen Anbietern du Kunde bist und wo wir nach deinem Tod Änderungen vornehmen sollen. Du teilst uns zum Beispiel deine Zugangsdaten von Facebook mit, die wir verschlüsselt speichern. Du gibst an, ob wir dein Konto später deaktivieren oder bestimmte Inhalte hochladen sollen. Wenn wir von der Steuerbehörde die Information bekommen, dass du gestorben bist, setzen wir deinen letzten Willen um.“[130] Die Kunden konnten festlegen, für wen ihr digitaler Nachlass bestimmt ist. MyWebwill war an das nationale amtliche Melderegister angeschlossen und wurde automatisch über Sterbefälle informiert, sodass Angehörige den Todesfall nicht melden und mit einer Sterbeurkunde nachweisen mussten. Erblasser mussten niemanden vorab über ihre Nachlassplanung informieren. Vermutlich hat aber das notwendige Hinterlegen sämtlicher Kennwörter und der nationalen (schwedischen) Personennummer bei MyWebwill manche potenziellen Nutzer davon abgehalten, einen solchen Dienst in Anspruch zu nehmen.

Ein weiteres Beispiel ist Perpetu, ein 2013 entstandener Dienst für digitale Nachlassplanung mit Sitz in Hongkong. Der Dienst verließ sich darauf, dass Online-Dienste wie Facebook, Twitter und Flickr beständig sind und den Nutzern wichtig bleiben. Beispielsweise wurden die Logos von Facebook, Twitter und Flickr verwendet,[131] um potenzielle Kunden anzusprechen, während vermutlich schon viele Nutzer von Flickr zu Instagram wechselten. Viele Social-Media-Dienste wie MySpace, Friendster, LiveJournal, GeoCities und andere sind inzwischen nicht mehr am Markt, sodass kein digitaler Nachlassdienst sich darauf verlassen kann, dass die Daten seiner Kunden auf der Plattform eines Drittanbieters erhalten bleiben. Kunden möchten nicht unbedingt Geld oder Zeit für ihren digitalen Nachlass aufwenden, wenn die Datenbasis selbst so vergänglich ist. MyWebwill, Perpetu, Legacy Locker, CirrusLegacy, Online Legacy, Entrustet, Lifestrand, Deathswitch and E-Z Safe sind Beispiele digitaler Nachlassdienste, die selbst sehr kurzlebig waren.

Der US-amerikanische Webdienst Get Your Shit Together (GYST)[132] versuchte, seine Nutzer dazu zu bringen, ihre digitale Nachlassplanung aktuell zu halten und mit alltäglichen Aktivitäten wie dem Zusammenstellen von Fotos, Videos, Zugriffsdaten und Checklisten zu verbinden. Der Dienst

[128] *Kneese*, Networked heirlooms: the affective and financial logics of digital estate planning, in: Cultural Studies 33.2, S. 297–324.

[129] *Brucker-Kley u. a.*, Sterben und Erben in der digitalen Welt: von der Tabuisierung zur Sensibilisierung, S. 66.

[130] https://www.dw.com/de/mein-letzter-internetwille-testament-online/a-5273253.

[131] Siehe https://www.startbase.hk/companies/perpetu

[132] Get Your Shit Together: https://getyourshittogether.org.

wurde 2019 von Cake aufgekauft, einer in Boston ansässigen Dienstplattform zur Nachlassplanung, die eng mit US-amerikanischen Unternehmen aus dem Gesundheitswesen, Finanzdienstleistern und Versicherungen zusammenarbeitet. Es scheint, als könnten digitale Nachlassdienste nicht ohne die Unterstützung durch etablierte Institutionen überleben. Die Langlebigkeit eines einzelnen digitalen Nachlasses bleibt fraglich, weil auch die Datenplattformen der Online-Dienstanbieter häufig kurzlebig sind. Damit kann ein einzelner Nachlassdienst allein kaum sicherstellen, dass die digitalen Werte jedes Nutzers als ein nachhaltig verknüpfter digitaler Nachlass weitergegeben werden können.[133]

Der niederländische Nachlassdienst Ziggur[134] bietet für die individuelle Nachlassplanung seinen Privatkunden u. a. Eingabemasken für die Wünsche im Sterbefall betreffend die persönlichen Profile bei Online-Dienstanbietern, darunter die drei Optionen „Keine Maßnahmen“, „Kontolöschung“ und „Gedenkzustand“. Mit der zusätzlichen Angabe „Geheimhaltung“ kann der Nutzer bestimmen, dass die Existenz eines Kontos im Sterbefall den Hinterbliebene nicht mitgeteilt werden soll. Mit der zugesagten Umsetzung der Wünsche unterstützt Ziggur eine Art „digitale Willensvollstreckung“, die an den Angehörigen und Erben vorbeigehen kann. Obwohl die Nutzer bei Ziggur keine Zugriffsdaten für die Online-Dienste hinterlegen, kann Ziggur diese Dienstleistungen anbieten, weil es mit den führenden internationalen Online-Dienstanbietern kooperiert. Die aktive Willensvollstreckung und die Registrierung im (niederländischen) Notariatsregister werden nur in der kostenpflichtige Variante angeboten.[135] Inzwischen nimmt Ziggur keine neuen Kunden mehr an,[136] sodass die Beständigkeit des Dienstes fraglich ist.

In Deutschland bietet der technische Dienstleister Columba[137] seit 2016 mit dem Web-Portal „QuickForm“ Bestattern und deren Kunden (Angehörige, Erben, Nachlassverwalter), Versicherungen, privaten und öffentlichen Partnern insbesondere die Möglichkeit, Abmeldungen bei Institutionen und Unternehmen einschließlich der Regelung des digitalen Nachlasses rein digital durchzuführen, sobald Columba die amtliche Sterbeurkunde des betreffenden Nutzers vorliegt. Den Hintergrund der Aktivitäten bildet eine laufend aktualisierte Datenbank mit nationalen und internationalen Adressen von Dienstanbietern. Viele Unternehmen – z. B. Rentenversicherungen, Krankenkassen, Versorgungsämter, ARD ZDF Deutschlandradio Beitragsservice, aber auch ausländische Dienste wie Facebook und Twitter – akzeptieren offenbar die über QuickForm erfolgten Mitteilungen der Sterbefälle, beenden ohne Eingabe von persönlichen Zugriffsdaten die betreffenden Vertragsverhältnisse bzw. führen die von den Erblassern und Erben gewünschte Übertragung und Fortsetzung der Verträge aus. Da Columba mit vielen Online- und Offline-Dienstanbietern kooperiert und auch komplexe Löschaufträge annimmt, lassen sich offenbar auch Aufträge durchführen (z. B. eine „unliebsame Mitgliedschaft“ löschen), ohne dass die Erben etwas davon erfahren.[138]

Fazit: Digitale Vererbungsdienste können für Erblasser und Erben hilfreiche Dienste anbieten, insbesondere, wenn diese Dienste von etablierten Institutionen und amtlichen Stellen unterstützt und von führenden Online-Dienstanbietern akzeptiert werden. Aus Nutzersicht gib es vor allem zwei Vorteile:

[133] *Kneese*, Networked heirlooms: the affective and financial logics of digital estate planning, in: Cultural Studies 33.2, S. 22.
[134] Ziggur: https://ziggur.me.
[135] *Brucker-Kley u. a.*, Sterben und Erben in der digitalen Welt: von der Tabuisierung zur Sensibilisierung, S. 76 ff.
[136] Siehe „U kunt geen nieuwe accounts meer aanmaken bij Ziggur“ auf https://ziggur.me/nl/home.aspx.
[137] Columba Online Identity Management AG: https://www.columba.de/de/digitaler-nachlass.
[138] *Wende*, Digitaler Nachlass – wie wir präventiv Regelungslücken vermeiden, in: Schmerzmedizin 35.2, S. 56.

Erstens brauchen Angehörige den Sterbefall nicht mit einer Sterbeurkunde gegenüber den Online-Dienstanbietern nachzuweisen – evtl. wird sogar der Vererbungsdienst automatisch über Sterbefälle benachrichtigt. Zweitens müssen die Vertrauenspersonen der nachlassplanenden Person nicht zwangsläufig vorab informiert werden, insbesondere dann nicht, wenn der Nachlassdienst zusätzlich und bei Bedarf die Erben unterstützt.

Das schwedische Beispiel MyWebwill zeigt, dass eine amtliche Unterstützung eines Dienstes nicht unbedingt gewährleistet, dass sich der Dienst dauerhaft etablieren kann. Eine Ursache des Scheiterns könnte darin liegen, dass die Nutzer ihre sämtlichen Kennwörter beim Dienst hinterlegen sollten. Warum sollten Nutzer einem Start-up-Unternehmen das Vertrauen entgegenbringen, dass ihre Zugriffsdaten nicht missbraucht werden und auch im Falle einer Dienstauflösung weiterhin geschützt sind? Andere Nachlassdienste verzichten weitgehend auf die Verwaltung von Zugriffsdaten und setzen vielmehr auf die direkte Zusammenarbeit mit den zuständigen Institutionen und den Online-Diensten.

Wichtige Anforderungen an die Nachlassdienste wären: Die Zuverlässigkeit und Langlebigkeit des Dienstes, die Sicherheit der hinterlegten Daten (insbesondere bei der Akkumulation von Zugriffsdaten), verbraucherfreundliche Nutzungsbedingungen und Datenschutzrichtlinien sowie die benutzungsfreundliche Bedienung. Ein Erfolgsfaktor von Nachlassdiensten scheint der Mehrwert zu Lebzeiten zu sein, beispielsweise eine Kombination mit einem digitalen Datensafe. Damit wird es wahrscheinlicher, dass die hinterlegten Daten von den Nutzern rechtzeitig aktualisiert werden.[139]

6.5.5.2 Rechtliche Bewertung

Auch die Verwendung digitaler Nachlassdienste ist – über die in Kapitel 6.5.6 auf der nächsten Seite vorgebrachten Einwände hinaus – kritisch zu beurteilen. So wird vorgebracht, dass es nie im Interesse des Erblassers liegen könne, wenn unbekannte digitale Nachlassverwalter Zugriff auf persönliche Daten erhalten.[140] Zudem müsse der Nutzer stark in Vorleistung treten, indem den Diensten – möglicherweise über Jahre hinweg – die Nutzungsgebühren zu zahlen und möglicherweise sensible Daten herauszugeben sind, damit nach ihrem Tod der Dienst genutzt werden kann. Dabei ist nicht sicher, ob es den Anbieter zu diesem Zeitpunkt noch gibt.[141]

Aus rechtspraktischer Sicht ist es jedoch jedenfalls vorteilhaft, wenn der Nachweis der Berechtigung (hinsichtlich Erbschaft oder Bevollmächtigung) durch die Begünstigten tatsächlich nur einmal gegenüber dem digitalen Nachlassdienst erbracht werden muss und nicht gegenüber jedem einzelnen Dienstanbieter. Dies ist beispielsweise offenbar hinsichtlich der Firma Columba der Fall, deren Angaben die Dienstanbieter akzeptieren. Fraglich ist jedoch, ob es im Vorfeld eine Garantie für die Nutzer gibt, dass die Abwicklung durch die Nachlassdienste im Vorsorgefall tatsächlich funktioniert.

[139] *Brucker-Kley u. a.*, Sterben und Erben in der digitalen Welt: von der Tabuisierung zur Sensibilisierung, S. 78 f.
[140] *Raude*, RNotZ 2017, S. 17 (23).
[141] *Seidler*, Digitaler Nachlass, S. 159.

Jedenfalls wird den Diensten auch zugutegehalten, dass sie lange vor der Rechtspraxis ein praktisches Problem erkannt und eine Lösung angeboten haben.[142] Zudem ist es ihnen gegebenenfalls durch ihre praktische Erfahrung und standardisierten Prozesse möglich, die Abwicklung erheblich zu beschleunigen. Vor allem IT-Dienstleister könnten – ähnlich wie ein Entrümpelungsservice – eine unterstützende Rolle für Berater und Erben spielen. Allerdings sind auch die digitalen Nachlassdienste häufig standardisiert und bieten Lösungen nur für die gängigen Plattformen an. Problematisch könnte dabei jedoch der Fall sein, wenn der Erblasser eine atypische Seite betreut oder verwendet, z. B. die des örtlichen Sportvereins. Zu beachten ist auch, dass die Anbieter nicht denselben Aufbewahrungspflichten und Verschwiegenheitspflichten wie Berufsträger unterliegen, sodass die Datensicherheit erneut fraglich ist. Hingewiesen wird daher darauf, dass aufgrund der vielfältigen Probleme eine rechtliche Begleitung der Nutzung digitaler Nachlassdienste zu empfehlen ist, da im jeweiligen Einzelfall geprüft werden muss, ob der jeweilige Anbieter, „hält, was er verspricht“ und insbesondere den Sicherheitsanforderungen genügt.[143]

Allerdings ist dann die Praktikabilität und Kostenersparnis für die Verbraucher fraglich, wenn nicht nur Kosten und Aufwand für den digitalen Nachlassdienst, sondern zudem für rechtliche Beratung aufgebracht werden müssen. Da die digitalen Nachlassdienste in ihrem Angebot und ihrer Funktionsweise jedoch sehr unterschiedlich sein können, muss wohl tatsächlich anhand des Einzelfalls geprüft werden, ob die Nutzung für die Verbraucher vorteilhaft ist.

Grundsätzlich steht es den Verbrauchern frei, einen digitalen Nachlassdienst als eine Art Nachlassverwalter hinzuzuziehen, wenn sie sich nicht selbst um die Abwicklung des digitalen Nachlasses kümmern wollen. Allerdings sollte es nicht die generelle Empfehlung sein, dass ein Dienstleister (zwingend) benötigt wird, um den Nachlass abzuwickeln. Es sollte – wie sonst im Rahmen der Nachlassabwicklung – grundsätzlich möglich sein, dass die Erben selbst die Abwicklung des Nachlasses durchführen können.

6.5.6 Generelle Kritik an kommerziellen Dienstanbietern

Soweit Dienste anbieten, Benutzerdaten auf ihrem Server oder in einer Cloud zu speichern (wie die meisten Passwort-Manager) und diese zusätzlich im Todesfall an die Erben weitergeben (wie die meisten digitalen Datensafes und einige digitale Nachlassdienste) wurde in der juristischen Literatur bereits wiederholt davon abgeraten, diese Dienste in Anspruch zu nehmen. Soweit die Tauglichkeit dieser Dienste zur technischen Unterstützung der Vorsorge angezweifelt wird,[144] sind die Kritikpunkte teilweise sehr ähnlich, weshalb diesbezüglich eine gemeinsame Darstellung erfolgen soll.

[142] *Herzog/Pruns*, Digitaler Nachlass, § 9 E Rn. 22.
[143] *Herzog/Pruns*, Digitaler Nachlass, § 9 E Rn. 23 f.
[144] *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1922 Rn. 385.

6.5.6.1 Datensicherheit

Zunächst werden grundsätzliche Bedenken hinsichtlich der Sicherheit der Daten vorgebracht.[145]

Soweit sämtliche Zugangsdaten auf dem Server des Anbieters oder in einer Cloud gespeichert sind, besteht stets die Gefahr, dass sich unbefugte Dritte, beispielsweise durch Hackerangriffe, Zugriff auf die Server verschaffen. Auch ist nicht sichergestellt, wie die Anbieter sich verhalten, wenn staatliche Stellen Zugriff auf die Daten verlangen.[146] Insgesamt kann nicht nachvollzogen werden, wie das Unternehmen die ggf. vertraulichen Daten handhabt, ob, wem und unter welchen Voraussetzungen die Daten herausgegeben werden oder Unberechtigte sich Zugang verschaffen können.[147]

Auch besteht eine hohe Missbrauchsgefahr,[148] da wohl durch die Verbraucher nie gänzlich sichergestellt werden kann, dass die Dienstanbieter die Daten nicht auch verwerten.[149] Jedenfalls ist der Handel mit Daten ein durchaus lukratives Geschäft.[150]

Somit kann der Verbraucher nie sicherstellen oder überprüfen, ob die Daten auf dem Server des Anbieters tatsächlich ausreichend gesichert sind.[151] Der Verbraucher trägt das Risiko für Schäden im Fall des Verlustes oder der Manipulation der Daten.[152]

Auch müsste der Verbraucher genau prüfen, wie im vertraglich vorgesehenen Fall – meist ist dies der Tod des Nutzers – die Herausgabe der Daten an die Begünstigten tatsächlich umgesetzt werden soll,[153] was wohl vor allem für rechtliche und technische Laien kaum durchführbar ist.

Darüber hinaus wird vorgebracht, dass die Herausgabe der Zugangsdaten an private Dienstleister der grundsätzlich gebotenen Geheimhaltung von Passwörtern widerspricht.[154]

Aus diesen Gründen wird grundsätzlich empfohlen, dass die einzelnen Zugangsdaten in eigener Hand bleiben sollten.[155]

---

[145] *Steiner/Holzer*, ZEV 2015, S. 266.
[146] *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ, S. 4 (10); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97; *Lange/Holtwiesche*, ErbR 2016, S. 487 (491); *Rott/Rott*, NWB-EV 2013, S. 160 (168); *Martini*, JZ 2012, S. 1145 (1154); *Kutscher*, Digitaler Nachlass, S. 150; *Seidler*, Digitaler Nachlass, S. 159.
[147] *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ, S. 4 (11 f.); *Lange/Holtwiesche*, ErbR 2016, S. 487 (491); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97; *Kutscher*, Digitaler Nachlass, S. 150.
[148] *Deusch*, ZEV 2014, S. 2 (7); *Seidler*, Digitaler Nachlass, S. 159.
[149] *Kutscher*, Digitaler Nachlass, S. 150.
[150] *Raude*, RNotZ 2017, S. 17 (23).
[151] *Bleich*, c't 2/2013, S. 62 (64); *Martini*, JZ 2012, S. 1145 (1154).
[152] *Deusch*, ZEV 2014, S. 2 (7).
[153] *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[154] *Martini*, JZ 2012, S. 1145 (1154).
[155] *Bleich*, c't 2/2013, S. 62 (64).

6.5.6.2 Keine staatliche Kontrolle der Dienste

Zudem gibt es bisher kein Zertifizierungsverfahren – Qualitätskontrolle, verlässliche Siegel oder gar staatliche Aufsicht[156] – dieser Dienstleistungen,[157] die eine Auswahl für die Verbraucher erleichtern würde. Es ist nicht sichergestellt, ob die Anbieter die versprochenen Leistungen auch tatsächlich erfüllen, also im Erbfall die Daten tatsächlich an die vorher bestimmten Personen herausgegeben werden, oder dass der Anbieter im Todesfall zuverlässig und vor allem rechtsverbindlich vom Todesfall Kenntnis erlangt.[158] Ähnliche Bedenken bestehen hinsichtlich des Eintritts der Handlungsunfähigkeit.

6.5.6.3 Insolvenzrisiko

Trotz dieser Risiken ist die Nutzung dieser Dienste je nach Anbieter für die Verbraucher mit erheblichen Kosten verbunden.[159]

Diesbezüglich kommt erschwerend hinzu, dass es sich häufig um Start-Up-Unternehmen handelt, deren Beständigkeit durchaus fraglich ist.[160] Insbesondere, wenn junge Verbraucher den Dienst für ihre Vorsorge nutzen und der Dienst somit über längere Zeit bestehen muss, besteht immer die Gefahr, dass der Dienst eingestellt wird oder Insolvenz angemeldet werden muss und so das Vertragsziel verfehlt wird,[161] weil die Zugangsdaten im Ernstfall nicht mehr abrufbar sind.[162] Insgesamt ist in diesem Fall das Schicksal der Daten unsicher,[163] insbesondere, ob diese auch nach Einstellung des Dienstes noch ausreichend gesichert sind.

Zudem wird darauf hingewiesen, dass eine Gefahr bestehe, dass ein Insolvenzverwalter sich die Herausgabe der Zugangsdaten an die Berechtigten noch einmal gesondert vergüten lässt und so zusätzliche Kosten auf die Verbraucher zukommen.[164]

6.5.6.4 Ergebnis

Anbieter, die Benutzerdaten speichern und anbieten, im Todesfall Daten an die Erben weiterzugeben, können daher wohl nur dann empfohlen werden, „wenn der Dienst dem Erblasser seine persönliche Integrität und dauerhafte wirtschaftliche und technische Leistungsfähigkeit nachgewiesen hat“,[165]

[156] *Martini*, JZ 2012, S. 1145 (1154).
[157] *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ 2015, S. 4 (11 f.); *Lange/Holtwiesche*, ErbR 2016, S. 487 (491); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97; *Kutscher*, Digitaler Nachlass, S. 150.
[158] *Raude*, RNotZ 2017, S. 17 (24).
[159] *Raude*, RNotZ 2017, S. 17 (23 f.).
[160] *Raude*, RNotZ 2017, S. 17 (23); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97.
[161] *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ 2015, S. 4 (11 f.); *Lange/Holtwiesche*, ErbR 2016, S. 487(491); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97; *Kutscher*, Digitaler Nachlass, S. 150; *Seidler*, Digitaler Nachlass, S. 159.
[162] *Gloser*, MittBayNot 2016, S. 101 (105); *ders.*, DNotZ 2015, S. 4 (10 f.); *Rott/Rott*, NWB-EV 2013, S. 160 (168).
[163] *Raude*, RNotZ 2017, S. 17 (24); *Martini*, JZ 2012, S. 1145 (1154); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 97.
[164] *Rott/Rott*, NWB-EV 2013, S. 160 (168).
[165] *Deusch*, ZEV 2014, S. 2 (7).

was zumindest unter den derzeitigen Voraussetzungen praktisch kaum durchführbar ist.

6.5.7 Zugangsdaten in lokalen Archiven und auf Papier

6.5.7.1 Technische Darstellung und Bewertung

Aus Unsicherheit darüber, ob Produkte und Online-Dienste des digitalen Nachlasses langfristig zuverlässig und ihre Kosten wert sind, suchen viele Nutzer nach eigenen Lösungen. So werden Dokumente, Passwörter und kryptografische Schlüssel eigenhändig auf externen Medien wie separaten Festplatten, CD-ROMs, DVDs oder USB-Sticks archiviert. Einige Quellen empfehlen, von den genutzten Online-Diensten wie Facebook, Twitter, YouTube, Google, Mail-Providern etc. regelmäßig die eigenen Daten herunterzuladen, diese Daten lokal auf separaten Festplatten zu archivieren und diese Archive regelmäßig zu aktualisieren. CD-ROMs, DVDs und Flash-Laufwerke werden nicht empfohlen, da die zugrundeliegenden Formate evtl. in einigen Jahren durch andere Formate ersetzt werden.[166] Ohne regelmäßige Aktualisierung auch des Speichermediums bleibt die Unsicherheit darüber, wie viele Jahre die Geräte noch lesbar bleiben, d. h. ob die Erben noch die archivierten Daten lesen können. Texte sollten in Form von einfachen ASCII-Textdateien archiviert werden.[167, 168] Darüber hinaus müssen die technischen Speichermedien für die Erben gut auffindbar hinterlegt werden. Grundsätzlich ist unklar, wie lang die darauf gespeicherten Daten stabil bleiben.[169] Da die Daten aber ohnehin aktuell gehalten werden müssen, sollten die Nutzer regelmäßig auch die Funktion des Speichermediums überprüfen. USB-Sticks haben den Vorteil, dass sie sehr weit verbreitet und leicht anwendbar sind. Es kann aber dennoch sein, dass sich nach einigen Jahren eine andere Technik durchsetzen wird. Umso wichtiger scheint es, dass der Nutzer das Speichermedium mit den Zugangsdaten zu Lebzeiten nicht aus der Hand gibt und es bei Bedarf durch eine neuere Technik ersetzt.

Im Rückblick scheint allerdings eine Archivierung in Papierform viel länger zugreifbar und lesbar zu sein als die digitalen Speichermedien der vergangenen Jahrzehnte. Da physische Aktenordner meist Teil eines Nachlasses sind und von den Angehörigen beachtet werden, liegt es nahe, darin auch die Daten des digitalen Nachlasses in Papierform zu hinterlegen, in der Erwartung, dass diese Informationen nicht ignoriert oder unbedacht fortgeworfen werden – anders als das bei USB-Sticks oder elektronischen Geräten befürchtet werden muss, da deren Zweck und gespeicherte Daten nicht auf den ersten Blick ersichtlich sind. Zumindest die Informationen über ggf. vorhandene digitale Archive sollten für Personen, die den Nachlass verwalten, auch in Papierform hinterlegt werden. Zu den notwendigen Informationen gehören beispielsweise, welche digitalen Archive existieren, wo diese zu finden sind und wie man auf die darin gespeicherten Daten zugreifen kann und genaue Anweisungen

[166] *Nagel u. a.*, Death and the Internet – Consumer issues for planning and managing digital legacies.

[167] The National Archives (UK): Selecting File Formats for Long-Term Preservation (2008), https://www.nationalarchives.gov.uk/documents/selecting-file-formats.pdf.

[168] ASCII enthält nur wenige Zeichen, die zur Texttrukturierung verwendet werden können. Verschiedene Betriebssysteme erwarten zudem jeweils andere ASCII-Zeichen am Zeilenende. Allgemein werden zur Textformatierung inzwischen eher Auszeichnungssprachen („Markup Languages“) wie HTML bevorzugt.

[169] Daten auf USB-Sticks sind evtl. nur wenige Jahre stabil, vgl. *Lutz Labs*, Sicher aufbewahren – Hardware und Medien für das persönliche Archiv, in: c't 8/2017, S. 114.

darüber, was mit den Daten nach dem Willen des Erblassers gemacht werden soll. Die archivierten Daten sowie die Informationen darüber sollten nicht direkter Teil eines Testaments oder einer Vorsorgevollmacht sein, da ansonsten auch unberechtigte Personen Einblick in die Daten bekommen könnten. Die Erstellung von Testament und Vorsorgevollmacht, kombiniert mit separat aufbewahrten Zugriffsdaten, gilt als die sicherste Art, Vorsorge für den digitalen Nachlass zu treffen.[170] Als Vorsorgemaßnahme wird dem Erblasser empfohlen, die folgenden Schritte durchzuführen:[171]

(1) **Festlegen des digitalen Nachlasses**: Zusammenstellung der digitalen Online-Konten und Daten, z. B. Social-Media-Profile, Domainnamen, Blogs, Websites, E-Mail-Konten, Anwendungssoftware, Spielkonten, Fotos und andere Dokumente.

(2) **Erstellen des digitalen Archivs**: Speicherung lokaler Backups von den eigenen Daten der Online-Konten auf lokalen Speichermedien. Sicherung der Daten durch Verschlüsselung und Passwörter. Getrennte Aufbewahrung der Schlüssel und Passwörter z. B. in Papierform mit Kopie für die Vertrauensperson.

(3) **Bestimmen von Vertrauensperson(en)**: Treffen einer Entscheidung darüber, wer den digitalen Nachlass verwalten soll. Diese Person sollte über die technischen Fähigkeiten verfügen, die Anweisungen in Bezug auf die Dateien auszuführen. Die Entscheidung könnte ggf. in das Testament aufgenommen werden. Die Vertrauenspersonen sollten ggf. möglichst mit den in den Online-Diensten hinterlegten Kontakten übereinstimmen.

(4) **Zusammenstellen von Metainformationen**: Angaben von Standorten, Zugriffsmethoden, Zugriffsdaten und Wünsche für den digitalen Nachlass. Dazu gehören unbedingt auch Zugriffsdaten zu Smartphone und Tablet (SIM-PIN, PUK, Sperrkennwort), die evtl. mit Online-Konten verknüpft sind (z. B. iPhone mit der Apple-ID). Es müssen Anweisungen gegeben werden, wie auf Daten und Konten zugegriffen werden kann und was mit ihnen geschehen soll (z. B. Auszahlung von finanziellen Beträgen, Löschung eines Kontos, Einrichtung einer digitalen Gedenkstätte). Sollen Konten weitergeführt werden, ist eine Zusammenstellung der dafür relevanten Vertragsbedingungen und durchzuführenden Schritte sinnvoll.

(5) **Vorbereiten des Schriftverkehrs**: Erstellen von Anschreiben, Beschreiben der dienstspezifischen formellen Verfahren zum Nachweis des Sterbefalls, z. B. ob und wie die Online-Dienstanbieter eine Sterbeurkunde oder einen veröffentlichten Nachruf erwarten, aber auch welche Person befugt ist, im Namen der verstorbenen Person zu handeln.

Das Zusammenstellen von Metainformationen könnte in Papierform in einer Weise erfolgen, die den Erben die Rückwandlung der Daten in eine digitale Form erleichtert. Neben dem Einscannen von normalem Text mit automatischer Texterkennung mittel OCR[172] können beispielsweise technische Zugriffsdaten wie längere Passwörter und kryptografische Schlüssel in Form von QR-Codes[173] auf

[170] *Funk*, Das Erbe im Netz: Rechtslage und Praxis des digitalen Nachlasses, S. 29.

[171] *Nagel u. a.*, Death and the Internet – Consumer issues for planning and managing digital legacies., S. 17 f.

[172] OCR („Optical Character Recognition“) dient der automatisierte Texterkennung aus Bildern und erzeugt digitale Textinformation.

[173] QR-Codes („Quick Response Codes“) sind zweidimensionale maschinenlesbare Codes aus schwarzen und weißen Quadraten, die die kodierten Daten binär darstellen.

Papier gedruckt werden. QR-Codes können mit einer Smartphone-Kamera leicht gelesen werden, d. h. die Nutzer brauchen die Daten bei Bedarf nicht händisch an der Tastatur einzugeben. Form und Bedeutung von QR-Codes sind zwar standardisiert, könnten aber mit den Jahren wiederum ihre Verbreitung verlieren und durch neuere Techniken ersetzt werden.

Vermutlich ist für den Ausdruck von komplexen technischen Daten (z. B. kryptografischen Schlüsseln) auf Papier die hexadezimale Darstellung der Daten am geeignetsten, da es sich um eine sehr elementare Darstellung von Zeichen handelt, die auch manuell abgeschrieben werden können und vermutlich noch sehr lange in Gebrauch sein wird. Eine automatische Wiederherstellung ist durch die Verwendung einer OCR-Software möglich. Geheime Daten können zunächst auf Basis eines Masterpassworts verschlüsselt werden, bevor sie ausgedruckt werden, um die manuelle Eingabe oder die automatische Digitalisierung des verschlüsselten Textes einem Dritten überlassen zu können, ohne dabei das Geheimnis preiszugeben. Anschließend könnten die Erben das Masterpasswort in eine lokale Anwendung eingeben, um die digitalisierten Daten zu entschlüsseln.[174]

Grundsätzlich findet aber auch bei dieser kombinierten Lösung aus digitalem Archiv und Papier keine Vorbereitung in dem Sinne statt, dass die betreffenden Online-Lösungsanbieter über die geplante Übergabe der Nutzerkonten informiert und in den Prozess miteinbezogen werden. Es handelt sich eher um eine Archivlösung, um Daten zu retten und Konten zu lokalisieren, nicht um Online-Konten weiterzuführen. Die Übergabe der Zugriffsdaten an die Erben könnte damit gut vorbereitet und erfolgreich ablaufen. Der Erblasser könnte zur Sicherheit bereits zu Lebzeiten die Übergabe der Archive und Zugriffsdaten durchführen, indem er die Daten den Erben anvertraut und ihnen den Zugriff auf Online-Konten ermöglicht. Dies ist allerdings nicht immer wünschenswert. Nach dem Tod des Erblassers müssten die Erben zur Weiterführung der Konten in jedem Fall weitere Schritte durchführen, die sich an den Vertragsbedingungen der Dienstanbieter orientieren.

Fazit: Erblasser könnten persönliche digitale Archive anlegen und die für die Erben wichtigen Informationen über den digitalen Nachlass in Papierform archivieren. Die Archive wären das digitale Analogon zur herkömmlichen Archivierung wichtiger Gegenstände etwas in Boxen oder Stahlkassetten. Die Metadaten auf Papier könnten zusammen mit anderen wichtigen Papieren wie Urkunden, Testament etc. für den Erbfall aufbewahrt werden. Die ausgedruckten Metadaten können auch technische Daten enthalten. Diese sollten dann aber möglichst redundant in verschiedenen Datenformaten abgedruckt sein, um eine sichere Speicherung und einfache Wiederherstellung der digitalen Daten mit mindestens einem der angewandten Verfahren zu ermöglichen. Mühsam wird das Verfahren für den Erblasser, wenn die Archivdaten und Metadaten zu Lebzeiten öfter aktualisiert werden müssen, insbesondere wenn es sich um verschlüsselte technische Zugriffsdaten (kryptografische Schlüssel) handelt, die nur schwierig manuell überprüft werden können. Prinzipiell bleiben alle Daten leicht und ohne Internetverbindung zugänglich. Wie die anderen genannten Vorsorgelösungen bezieht auch diese Lösung die Online-Dienstanbietern nicht systematisch in die Vorsorge mit ein.

[174] Das Fraunhofer SIT hat zum Thema „Langzeitsicherung von kryptografischen Schlüsseln auf Papier mit benutzungsfreundlicher Wiederherstellung der digitalen Daten“ technische Konzepte und eine prototypische Software entwickelt, die allerdings noch nicht veröffentlicht sind.

6.5.7.2 Rechtliche Bewertung

Es besteht grundsätzlich die Möglichkeit, eine privatschriftliche Liste mit sämtlichen Zugangsdaten anzufertigen. Zu beachten ist, dass sich eine solche Liste nicht direkt in einer letztwilligen Verfügung oder einer Vorsorgevollmacht befindet, sondern ein separates Dokument angefertigt werden sollte. Dies wird auch als „digitale Vorsorgemappe“[175] bezeichnet.

Verlust der Liste

Um den Begünstigten die Zugangsdaten zur Verfügung zu stellen, ist die Auflistung sämtlicher Zugangsdaten auf Papier und die Aufbewahrung dieses Dokuments zu Hause grundsätzlich möglich. Auch hiervon wird in der Regel jedoch abgeraten. So besteht zunächst die Gefahr eines unberechtigten Zugriffs durch Dritte. Dies können sowohl Einbrecher als auch sämtliche Personen sein, die Zugang zum Haus des Verbrauchers haben. Insoweit ist wohl auch ein Haftungsrisiko des Nutzers für rechtswidrige Handlungen und durch den Dritten geteilte Inhalte nicht auszuschließen,[176] da es sich um sehr sensible Daten handeln kann.[177] Daneben besteht eine Gefahr des Verlusts der Liste, sei es durch Brand- oder Wasserschäden[178] oder durch bloßes Verlegen.[179]

Von anderer Seite wird die Auflistung der Passwörter auf handschriftlichen Listen jedoch als legitime Möglichkeit anerkannt. Zugegebenermaßen ist dies wohl jedenfalls sicherer als die Hinterlegung auf dem Server eines Online-Dienstes. Aus dem Internet zugängliche Passwörter sind einem Missbrauch durch einen größeren Personenkreis ausgesetzt, als zu Hause aufbewahrte handschriftliche Listen. Insoweit wird die Situation mit der Aufbewahrung von Schlüsseln verglichen.[180] So kann eine handschriftliche Liste geeignet sein, wenn dem Verbraucher in seinem Haus ein geeigneter Ort zur Aufbewahrung zur Verfügung steht und er nicht befürchtet, dass Unberechtigte darauf Zugriff nehmen.

Jedenfalls ist eine handschriftliche Liste aber wohl nicht die sicherste Alternative für die Aufbewahrung von Zugangsdaten.

Gesamte Liste an Vertrauensperson

Aufgrund der Bedenken, die gegen eine Aufbewahrung der digitalen Vorsorgemappe im eigenen Aktenschrank vorgebracht werden, wurde daneben vorgeschlagen, einer Vertrauensperson eine Liste über die Online-Vertragsbeziehungen samt Benutzernamen und Passwörtern zu übergeben.[181]

Durch die Hinterlegung bei einer privaten Vertrauensperson oder einem Freund könnte zwar die Gefahr des unberechtigten Zugriffs durch Erben eingeschränkt und Kosten gespart werden. Allerdings

[175] So auch *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 75.
[176] *Salomon*, NotBZ 2016, S. 324 (328).
[177] *Steiner/Holzer*, ZEV 2015, S. 262 (265 f.); *Gloser*, MittBayNot 2016, S. 101 (106).
[178] *Gloser*, MittBayNot 2016, S. 101 (105).
[179] *Raude*, RNotZ 2017, S. 17 (24 f.); *Salomon*, NotBZ 2016, S. 324 (328); *Rott/Rott*, NWB-EV 2013, S. 160 (167 f.).
[180] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 13.
[181] *Deusch*, ZEV 2018, S. 687 (691); dies soll ausdrücklich dazu dienen den Providern im Ernstfall zuvorkommen zu können.

ist dagegen vorzubringen, dass die Vertrauensperson große Verantwortung hinsichtlich der Zugangsdaten trägt und auch ein Haftungsrisiko im Fall des Verlusts der Liste treffen würde.[182] Auch müsste bei jeder Passwortänderung oder wenn neue Zugangsdaten hinzukommen, die Vertrauensperson aufgesucht und die Liste ergänzt werden, was zumindest Disziplin erfordert und relativ aufwendig ist.

Jedenfalls aus haftungsrechtlicher Sicht kann man aber wohl keiner Privatperson raten, eine solche Liste an sich zu nehmen. Zudem ist hinsichtlich der Hinterlegung bei einer privaten Vertrauensperson das Missbrauchsrisiko nicht kalkulierbar.[183]

So wurde stattdessen die Hinterlegung der gesamten Liste in einem Bankschließfach,[184] beim Nachlassgericht oder bei einem Notar vorgeschlagen, um die Sicherheit der Daten zu gewährleisten. Dagegen wird jedoch zu Recht vorgebracht, dass diese Lösung recht unpraktikabel sei. Zunächst ist die Hinterlegung von Nachlassdokumenten oder Vollmachten in einem Bankschließfach häufig deshalb nicht geeignet, da nur die berechtigte Person im Ernstfall überhaupt Zugang zu dem Schließfach erhält. Jedenfalls ist also davon abzuraten, letztwillige Verfügungen oder Vollmachten dort aufzubewahren, die zur Legitimation des Begünstigten benötigt werden.[185] Befindet sich allerdings allein die digitale Vorsorgemappe im Bankschließfach, hängt von dieser nicht die Legitimation gegenüber der Bank ab, sodass in der Regel keine Zugangsprobleme bestehen sollten.

Allerdings sind nach der allgemeinen Empfehlung Passwörter regelmäßig zu ändern. Befindet sich eine Liste mit sämtlichen Zugangsdaten inklusive Passwörtern jedoch in einem Bankschließfach oder bei einem Notar, führt die Änderung des Passworts insofern zu praktischen Schwierigkeiten, als zugleich auch jedes Mal die Liste geändert werden müsste. Für jede dieser Änderungen müsste ein Termin vereinbart werden, der – zumindest auf Dauer – mit erheblichen Kosten, Aufwand und praktischen Schwierigkeiten für den Verbraucher verbunden ist.[186] Dieselbe Problematik stellt sich, wenn neue Vertragsbeziehungen abgeschlossen werden und neue Zugangsdaten der Liste hinzuzufügen sind.[187]

Insbesondere in der von Notaren geprägten Literatur wird gegen eine Verwahrung sämtlicher Passwörter bei einem Notar zudem die drohende Überlastung der Notare vorgebracht. Darüber hinaus bestünde immer die Gefahr von Lagerungsschäden. Für die Verbraucher käme erschwerend hinzu, dass sie genaue Anweisungen für die Lagerung der Daten geben müssten.[188]

[182] *Deusch*, ZEV 2014, S. 2 (7).
[183] *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[184] Vorgeschlagen bei *Deusch*, ZEV 2014, S. 2 (7); *Bleich*, c't 2/2013, S. 62 (64).
[185] *Rott/Rott*, NWB-EV 2013, S. 160 (167 f.).
[186] *Rott/Rott*, NWB-EV 2013, S. 160 (168); *Deusch*, ZEV 2014, S. 2 (7); *Raude*, RNotZ 2017, S. 17 (25); *Lange/Holtwiesche*, ErbR 2016, S. 487 (491); *Gloser*, MittBayNot 2016, S. 101 (106); *Steiner/Holzer*, ZEV 2015, S. 262 (265).
[187] *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[188] *Gloser*, DNotZ 2015, S. 4 (15).

6.5.8 Zugangsdaten in digitaler Vorsorgeurkunde

Aufgrund dieser verschiedenen Bedenken wird – mittlerweile fast einhellig – die unter dem Begriff „digitale Vorsorgeurkunde“ zusammengefasste Konstruktion empfohlen. Zwar wird dies zumeist im Rahmen des Nachlassfalles diskutiert. Die digitale Vorsorgeurkunde eignet sich jedoch auch für den Fall des Eintritts der Hilfsbedürftigkeit.

Dabei soll die Liste der Zugangsdaten verschlüsselt auf einem lokalen Datenträger, wie einem USB-Stick oder einer Festplatte,[189] gesichert werden. Die Verschlüsselung soll mit einem Masterpasswort, das in sonst keinem anderen Zusammenhang verwendet wird, gesichert werden.[190] Zur Verschlüsselung der Daten wurde bereits wiederholt die Verwendung des Passwort-Managers KeePass vorgeschlagen.[191]

Das Masterpasswort – und im Fall der Verwendung von KeePass auch das Notfallblatt – soll einer Vertrauensperson übergeben werden. Als eine derartige Vertrauensperson wird aufgrund der oben beschriebenen Bedenken keine Privatperson, sondern eine Person vorgeschlagen, die beruflich zur Verschwiegenheit verpflichtet ist, wie ein Notar, Steuerberater oder Rechtsanwalt.[192] Allerdings ist die Aufbewahrung durch eine Privatperson dann möglich, wenn der Verbraucher das notwendige Vertrauen in diese Person hat.

Im Fall der Verwahrung durch einen Notar kann das Masterpasswort in einer Anlage zur sogenannten notariellen digitalen Vorsorgeurkunde vermerkt werden. Diese stellt eine Ergänzung zu einer Vorsorgevollmacht oder einer letztwilligen Verfügung dar.[193] Zu beachten ist, dass die sogenannte Vorsorgeurkunde nie eine materielle Ermächtigung durch Vollmacht i. S. d. § 166 II 1 BGB oder eine erbrechtliche Verfügung sein, sondern diese nur unterstützend begleiten kann, da sie nur die tatsächliche Zugriffsmöglichkeit auf Benutzernamen und Passwörter ermöglicht.[194] Daher handelt es sich auch nicht um eine Beurkundung von Willenserklärungen, sodass eine Niederschrift gemäß §§ 36 ff. BeurkG ausreichend ist.[195]

Der Vorsorgeurkunde sind konkrete Handlungsanweisungen i. S. d. § 51 I Nr. 2, II BeurkG an den Notar beizufügen, wann, an wen und unter welchen Voraussetzungen eine Herausgabe erfolgen soll.[196] Diese Handlungsanweisungen sollten so klar, unmissverständlich und eindeutig sein, dass der Notar ohne Prüfung materiell-rechtlicher Anforderungen rein anhand formaler Voraussetzungen rechtlich sicher prüfen kann, ob die Herausgabe erfolgen kann. Damit das Masterpasswort selbst nicht in der EDV des Notars erscheint und somit für Dritte sichtbar werden könnte, wird empfohlen, zumindest

[189] *Steiner/Holzer*, ZEV 2015, S. 266.
[190] *Rott/Rott*, NWB-EV 2013, S. 160 (167 f.); *Salomon*, NotBZ 2016, S. 324 (329 f.).
[191] *Bleich*, c't 2/2013, S. 62 (64); *Gloser*, DNotZ 2015, S. 4 (13); *ders.*, MittBayNot 2016, S. 101 (106); *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 14.
[192] *Rott/Rott*, NWB-EV 2013, S. 160 (167 f.).
[193] *Raude*, RNotZ 2017, S. 17 (26).
[194] *Salomon*, NotBZ 2016, S. 324 (330 f.); *Gloser*, DNotZ 2015, S. 4 (11).
[195] *Salomon*, NotBZ 2016, S. 324 (330 f.).
[196] *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 83b; *Raude*, RNotZ 2017, S. 17 (25); *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 17; sehr ausführlich zu den Handlungsanweisungen *Gloser*, DNotZ 2015, S. 4 (16 ff.); *ders.*, MittBayNot 2016, S. 101 (106).

das Masterpasswort nur in einer Anlage zur Urkunde beizufügen.[197] Die Anlage könnte auch durch den Erblasser bzw. Vollmachtgeber selbst ausgefüllt werden.[198]

Sollen verschiedene Zugangsdaten verschiedenen Personen zukommen, besteht die Möglichkeit, mehrere Masterpasswörter in verschiedenen Anlagen der notariellen Niederschrift beizufügen. Es ist jedoch zu beachten, dass auch die Liste der Zugangsdaten so zu sichern ist, dass die Masterpasswörter nur Zugang zu den jeweils zugewendeten Zugangsdaten ermöglichen.[199]

Dieses Masterpasswort sowie die genauen Handlungsanweisungen für den Notar werden in die notarielle Niederschrift aufgenommen.

Der lokale Datenträger, auf dem sich die verschlüsselte Liste der Zugangsdaten befindet, soll im Besitz des Erblassers bzw. Vollmachtgebers verbleiben und an einem im Ernstfall für die Begünstigten zugänglichen Ort aufbewahrt werden.[200] Dadurch kann auch die Geheimhaltungspflicht des Nutzers hinsichtlich seiner Passwörter gewahrt bleiben, da nur er bis zum Eintritt des Vorsorgefalls die tatsächlichen Passwörter kennt.[201] Dem Nutzer ist es so auch einfach möglich, auf dem lokalen Datenträger wie empfohlen die Passwörter regelmäßig zu aktualisieren oder neue Zugangsdaten zu ergänzen. Der Notar verwahrt nur das Masterpasswort, durch das der lokale Datenträger gesichert ist, und muss in diesen Vorgang nicht jedes Mal einbezogen werden.[202]

Das bei einem Notar hinterlegte Masterpasswort muss nicht so häufig aktualisiert werden. Dieses wird nur für die Sicherung des lokalen Datenträgers verwendet und nicht im sonstigen Rechtsverkehr. Somit ist das Passwort auch nicht auf den Servern von Dienstanbietern hinterlegt, weshalb der unbefugte Zugriff Dritter in geringerem Maße droht. Aus diesem Grund muss wohl eine Aktualisierung aus Sicherheitsgründen seltener erfolgen.[203]

Auch der lokale Datenträger und die Vorsorgeurkunde samt Anlagen sind sicher zu verwahren. Vorteil der notariellen Verwahrung ist jedoch, dass Notare an die Vorschriften der BNotO hinsichtlich der Verwaltung von Notarstellen und der Aufbewahrung von Akten gebunden sind, sodass auch die Gefahr von Lagerungsschäden gering ist.[204] Vorteil der notariellen Verwahrung gegenüber anderen Möglichkeiten der Verwahrung – insbesondere durch Privatpersonen und kommerzielle Dienstanbieter – ist auch, dass Notare gemäß § 18 BNotO verpflichtet sind, die Daten vertraulich zu behandeln. Die Geheimhaltung der Daten ist durch die für den Notar geltenden Datenschutzbestimmungen und die Verschwiegenheitspflicht sichergestellt.[205] Somit ist die Gefahr des unberechtigten Zugriffs Dritter und damit auch das Haftungsrisiko des Verbrauchers möglichst gering gehalten. Zudem ist durch die

[197] *Raude*, RNotZ 2017, S. 17 (25); *Salomon*, NotBZ 2016, S. 324 (329 f.); *Gloser*, DNotZ 2015, S. 4 (13); *ders.*, MittBayNot 2016, S. 101 (106); *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 16.
[198] *Gloser*, DNotZ 2015, S. 4 (14).
[199] *Salomon*, NotBZ 2016, S. 324 (329); *Raude*, RNotZ 2017, S. 17 (25).
[200] *Raude*, RNotZ 2017, S. 17 (25).
[201] *Rott/Rott*, NWB-EV 2013, S. 160 (167 f.).
[202] Statt aller hier *Bleich*, c't 2/2013, S. 62 (64); *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).
[203] *Raude*, RNotZ 2017, S. 17 (25); *Biermann*, in: Scherer (Hrsg.), Münchener Anwaltshandbuch Erbrecht, § 50 Rn. 76.
[204] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 16.
[205] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 16; *Raude*, RNotZ 2017, S. 17 (25).

Verwahrung bei einem Notar auch garantiert, dass die Daten dauerhaft gesichert sind[206] und so die Vorsorge Wirksamkeit erlangen kann.[207]

Die Aufbewahrung des lokalen Datenträgers sollte jedoch ebenfalls sorgfältig erfolgen.[208] Der Datenträger sollte so aufbewahrt werden, dass die Berechtigten im Vorsorgefall Zugriff auf ihn nehmen können, beispielsweise, indem der Datenträger in den persönlichen Unterlagen verwahrt wird, oder sichergestellt ist, dass der verschlüsselte Datenträger bereits zu Lebzeiten an die später Berechtigten übermittelt wird. Letzteres ist dann denkbar, wenn der Datenträger so ausreichend verschlüsselt ist, dass ein vorzeitiger Zugriff auf die Daten nicht möglich ist, sondern erst, wenn im Vorsorgefall das Masterpasswort mitgeteilt wird.[209] Bewahrt der Nutzer den lokalen Datenträger bei sich auf, kann die Information, wo dieser aufbewahrt wird, in die Vorsorgeurkunde aufgenommen werden.[210]

Die Lagerung sollte auch sicherstellen, dass unberechtigte Dritte nicht an den Datenträger gelangen. Auch vor einem Zugriff Unberechtigter sind die Daten aber durch ihre Verschlüsselung geschützt. Jedenfalls muss der Datenträger aber vor Lagerungsschäden geschützt werden.[211] Es ist auch zu beachten, dass digitale Datenträger nur eine begrenzte Lebensdauer aufweisen. Bewahrt der Nutzer den Datenträger jedoch bei sich auf, kann bei technischen Problemen oder in bestimmten Zeitintervallen ein Austausch mit einem funktionstüchtigen Gerät erfolgen.[212] Zuzugeben ist, dass es eine gewisse Disziplin vom Verbraucher erfordert, die Passwörter auf dem lokalen Datenträger und den Datenträger selbst regelmäßig zu aktualisieren.[213]

Auch ist die Hinterlegung der Vorsorgeurkunde bei einem Notar mit Kosten für den Verbraucher verbunden.[214] So besteht die Möglichkeit, über die Herausgabe an Dritte weitere Niederschriften zu erteilen und diese Urkunden mit der Haupturkunde zu verbinden. Auf diese Weise bleibt nachvollziehbar, wer Zugangsdaten erhalten hat und wie sich die Begünstigten legitimiert haben. Dies ist zwar zu Beweiszwecken günstig, allerdings verursacht diese Lösung zusätzliche Kosten. Aus Sicherheitsgründen ausreichend wäre insoweit wohl auch ein Erteilungsvermerk.[215]

Kosten lassen sich hinsichtlich der notariellen Verwahrung zwar nicht gänzlich vermeiden. Es trifft den Notar jedoch eine Pflicht, über die verschiedenen Möglichkeiten zu beraten. So können die Kosten auch dadurch gering gehalten werden, dass hinsichtlich des Masterpassworts keine Niederschrift nach §§ 36 ff. BeurkG erfolgt, sondern stattdessen das Masterpasswort auf einem Blatt Papier mit vom Notar beglaubigter Unterschrift in den Unterlagen des Notars hinterlegt wird.[216] Auch bleiben die Kosten insofern transparent, als diese durch die Notare nicht willkürlich festgesetzt werden, sondern sich nach der Gebührenordnung für Notare richten.

[206] *Raude*, RNotZ 2017, S. 17 (25).
[207] *Gloser*, DNotZ 2015, S. 4 (11).
[208] *Seidler*, Digitaler Nachlass, S. 160.
[209] *Gloser*, DNotZ 2015, S. 4 (15).
[210] *Steiner/Holzer*, ZEV 2015, S. 266.
[211] *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 83b; *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 14.
[212] *Raude*, RNotZ 2017, S. 17 (25).
[213] *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 83a.
[214] *Seidler*, Digitaler Nachlass, S. 159.
[215] *Raude*, RNotZ 2017, S. 17 (25).
[216] *Herzog/Pruns*, Digitaler Nachlass, § 9 D Rn. 15.

Strittig ist, ob der Notar verpflichtet ist, zu überprüfen, ob der konkrete Nutzungsvertrag die Übergabe des Passworts an ihn zulässt und den Notar diesbezüglich eine Hinweispflicht an den Verbraucher trifft,[217] oder ob der Verbraucher selbst prüfen muss, ob berufliche oder vertragliche Verbote der (mittelbaren) Weitergabe der Zugangsdaten durch die Vorsorgeurkunde entgegenstehen.[218] Insoweit steht jedoch auch die Wirksamkeit derartiger AGB infrage.[219]

6.5.9 Zentrale Plattform für amtliche Urkunden

6.5.9.1 Technische Darstellung und Bewertung

Als Alternative zu den genannten Vorsorgemaßnahmen – insbesondere zu den digitalen Datensafes in der Obhut von Privatpersonen und privatwirtschaftlichen Dienstanbietern – wäre ein zentrales Register unter staatlicher Obhut zur Ablage von digitalen Nachlassurkunden und anderen Nachweisen, auf die auch die betreffenden Online-Dienste zugreifen könnten. Dieses Register könnte ähnlich dem geplanten staatlichen Organspenderegister gestaltet sein oder zusammen mit Organspendeausweisen, Patientenverfügungen etc. in das Zentrale Vorsorgeregister oder das Zentrale Testamentsregister der Bundesnotarkammer aufgenommen werden. Dadurch hätten die Online-Dienstanbieter zumindest die Chance, sich vorab oder im Sterbefall des Erblassers über die Wünsche des Erblassers, z. B. eine geplante Kontenübergabe, zu informieren. Gäbe es entsprechende Nachlassformulare der Dienstanbieter, könnten diese ausgefüllt und unterschrieben in die Nachlassurkunden aufgenommen werden.

Es gibt bereits Forschungsansätze mit dem Ziel, die gesamten digitalen Daten einer Person über einen zentralen Cloud-Dienst als plattformübergreifende Sicherung von persönlichen Online-Dokumenten zugänglich zu machen. Demnach könnten über Softwareerweiterungen („Plugins“) Daten der Online-Dienste wie Facebook, Twitter, E-Mail zu einer zentralen Plattform geschafft werden. Dabei sollen auch die gesetzlich geregelte Übertragung eines digitalen Nachlasses (einschließlich notarieller Mitwirkung), die sichere Langzeitarchivierung und die Volltextsuche berücksichtigt werden.[220]

Ein systemtechnischer Lösungsansatz, die sogenannte „Plattform zur Vererbung von Digitalen Accounts“ (PVDA),[221] verfolgt das Ziel, die gesetzlichen Vorgaben des Erbrechts zu berücksichtigen und sieht dafür u. a. Folgendes vor: Starke Identitätsprüfungen der Nutzer (Online-Ausweisfunktion oder Postident-Verfahren), Meldung von Todesfällen auf rechtlich gesicherte Art (z. B. durch Nachlassgericht, Arzt oder Bestatter in Abgrenzung zum amerikanischen Prinzip selbstkonfigurierbarer DeathSwitches), Ausgabe von Mitgliedsausweisen zur Identifizierung ihrer PVDA-Konten und Einbezug von Cloud-Lösungen bei möglichst dezentraler Speicherung der Dokumente auf mobilen Endgeräten. Aus Gründen der Langzeitarchivierung sollen ausschließlich Dokumente im PDF/A-Format

[217] *Raude*, RNotZ 2017, S. 17 (25).
[218] *Gloser*, MittBayNot 2016, S. 101 (106).
[219] Siehe zur Prüfung von AGB ausführlich Kapitel 5 auf Seite 115
[220] *Pimminger u. a.*, Themis – Conserve your digital life.
[221] *Schmid u. a.*, Sterben im Internet – Regelung des digitalen Nachlasses, in: Wirtschaftsinformatik & Management 5.1, S. 86–96.

gespeichert werden, die zudem qualifiziert elektronisch signiert werden. Im Portal können digitale Dokumente, z. B. Organspendeausweise, Patientenverfügungen, Testamente, Sterbeurkunden, Erbscheine und persönliche Anweisungen zum digitalen Nachlass hinterlegt werden. Die Erben können die Informationen nutzen, herunterladen und ausdrucken und schließlich das geerbte Benutzerkonto löschen lassen.

In einer neueren Veröffentlichung wird auf Grundlage einer solchen PVDA ein staatlich geführtes Portal – beispielsweise unter der Obhut des BfDI – vorgeschlagen.[222] Diese Portalvariante soll die Erben von der Abwicklung des digitalen Nachlasses entlasten, dadurch dass Sterbeurkunden nach ihrer Ausstellung automatisch an das Portal übertragen und die Information darüber an die Online-Dienstanbieter übermittelt werden. Die Erblasser müssen zu Lebzeiten auf dem Portal ihre Online-Konten eintragen, samt betreffender E-Mail-Adresse und ggf. genutztem Pseudonym, aber ohne Angabe von Zugriffsdaten. Infolge der Benachrichtigung über den Sterbefall sollen die Online-Dienstanbieter gemäß der getroffenen Auswahl durch den Erblasser eine der folgenden drei Option umsetzen:

Option A.: **Löschung**: Das Konto wird im Sterbefall gelöscht, ohne dass jemand noch Zugang zu den Daten erhält.

Option B.: **Archivierung**: Das Konto wird eingefroren, Personen, die zuvor Zugang hatten (z. B. Freunde im sozialen Netzwerk) können aber weiterhin die Daten sehen. Möglicherweise kann eine Gedenkseite gezeigt oder eine Gedenkstätte eingerichtet werden.

Option C.: **Übergabe**: Das Konto wird an die vom Erblasser zu Lebzeiten eingetragenen Vertrauenspersonen übertragen, damit diese die Daten einsehen und verwalten können.

An die Dienstanbieter wird die Empfehlung gerichtet, die Nutzeroberfläche ihrer Dienste so zu gestalten, dass die genannten drei Optionen der digitalen Nachlassregelung dem Nutzer zur Auswahl stehen. Nur in den Fällen, in denen Nutzer zu Lebzeiten keine Auswahl treffen, soll die gesetzliche Erbfolge im Todesfall in Kraft treten. Die Autoren räumen ein, dass noch viele Fragen offen sind, beispielsweise Fragen zur Durchsetzbarkeit und zum Betrieb eines solchen Portals bis hin zu den rechtlichen Grundlagen für ein solches „Online-Testament“.

Fazit: Eine zentrale, staatlich unterstützte Plattform zur Nachlassverwaltung würde den Erblassern verbindliche Vorsorgemaßnahmen erleichtern und den Erben die Erbringung von Nachweisen vereinfachen. Hilfreich wäre beispielsweise ein Vermerk im amtlichen Personenstandsregister, dass eine digitale Nachlassplanung existiert und ggf. wo diese hinterlegt ist (z. B. bei einem bestimmten Notar oder Nachlassdienst). Allerdings wurde eine solche Plattform bisher nicht realisiert, da viele der damit verbundenen organisatorischen und rechtlichen Fragen noch ungeklärt sind und zudem Datenschutzbedenken hinsichtlich einer zentralen Speicherung von personenbezogenen Daten bestehen. Auch die vorausgesetzten technischen Schnittstellen existieren teilweise noch gar nicht. Schließlich sind die Dienstanbieter in die bestehenden Lösungsansätze nur unzureichend einbezogen.

[222] *Nellius/Zepic/Krcmar*, Finaler Logout – ein neuer Ansatz für die Gestaltung des digitalen Nachlasses bei sozialen Netzwerken, in: Digitalisierung von Staat und Verwaltung

6.5.9.2 Rechtliche Bewertung

Für die rechtliche Bewertung ist zwischen der Erweiterung des Zentralen Testamentsregisters bzw. des Zentralen Vorsorgeregisters und den Vorschlägen zur Schaffung einer PVDA zu unterscheiden.

Insbesondere der neueste Lösungsansatz zu einer PVDA[223] ist kritisch zu untersuchen, da die Argumentation des BGH zum digitalen Nachlass dort bereits berücksichtigt werden konnte. Zunächst ist dieser Lösungsvorschlag auf die Übertragung von Nutzerkonten bei sozialen Netzwerken beschränkt. Insofern könnte eine begriffliche Erweiterung angedacht werden, um den Lösungsansatz auf sämtliche Nutzerkonten des Erblassers auszudehnen. Dies gilt vor allem vor dem Hintergrund, dass so auch Nutzerkonten umfasst werden könnten, die finanzielle Interessen betreffen, und an denen die Erben somit nicht lediglich ein ideelles, sondern auch ein monetäres Interesse haben.

Grundsätzlich ist jedoch zunächst klarstellend festzuhalten, dass der Lösungsansatz – entgegen seiner eigenen Diktion – nicht eine erbrechtliche Vorsorge betrifft, sondern eine vertragliche Lösung zwischen Erblasser und Dienstanbieter darstellt. Die grundlegende Regelung, was mit dem Nutzerkonto nach dem Versterben geschehen soll, setzt eine Zusammenarbeit von Dienstanbieter und Nutzer voraus. Zwar betrifft die Regelung einen Zeitpunkt nach Versterben des Nutzers. Allerdings erfolgt dies nicht über erbrechtliche Regelungen, die einseitig und ohne Einbeziehung des Dienstanbieters möglich sind, sondern durch zwei übereinstimmende Willenserklärungen der Vertragsbeteiligten darüber, was mit dem Nutzerkonto nach Versterben des Nutzers geschehen soll und somit durch Vertrag. Selbst wenn es sich um eine erbrechtliche Regelung handeln würde, wäre diese formunwirksam, da auf dem vorgeschlagenen Weg keine testamentarische Regelung getroffen werden kann. Die grundsätzliche Vereinbarung geschieht somit – ohne Mitwirkung des Portals – vertraglich zwischen Nutzer und Dienstanbieter.

Das vorgeschlagene Portal leistet insofern im Sterbefall noch zweierlei. Einerseits werden die jeweiligen Dienstanbieter, hinsichtlich derer Nutzernamen bei dem Portal hinterlegt sind, automatisch und ohne Mitwirkung der Erben vom Todesfall benachrichtigt. Daraufhin sollen die Dienstanbieter die vertraglich vereinbarten Maßnahmen durchführen. Andererseits soll durch das Portal die Anonymität der Nutzer gewahrt werden, wenn sich diese mit einem Pseudonym bei dem sozialen Netzwerk angemeldet haben.
Letzteres ist jedoch infrage zu stellen. Zunächst ist anzuzweifeln, dass die Wahrung der Anonymität tatsächlich umfassend sichergestellt ist. Wählt der Nutzer die dritte Option der Benennung eines Nachlasskontakts, so ist zu beachten, dass zumindest dieser mit Vor- und Nachnamen sowie Geburtsdatum anzugeben ist. Der Nachlasskontakt kann somit nicht gegenüber dem Dienstanbieter anonym bleiben. Als Vertrauensperson werden jedoch wohl häufig Familienmitglieder gewählt, da eine Überlassung des Nachlasses regelmäßig innerhalb der Familie stattfindet, sodass auf diese Weise zumindest Rückschlüsse auf die Person des Nutzers gezogen werden könnten. Darüber hinaus muss eine eindeutige Identifikation des Nutzers zumindest gegenüber dem Portal erfolgen. Jedenfalls innerhalb dieser Beziehung ist somit die Anonymität nicht gewahrt. So könnten auch andere öffentliche

[223] *Nellius, u.a.*, Finaler Logout, in: *Räckers u. a.* (Hrsg.), Digitalisierung von Staat und Verwaltung, S. 37 ff.

Stellen (Staatsanwaltschaft, Polizei oder Verfassungsschutz) Auskunft von der Portal-führenden Stelle verlangen, um die Identität von Personen zu ermitteln, die im Internet über ein Pseudonym agieren. Bei Geltendmachung eines entsprechenden Informationsinteresses könnte das Portal diese Auskunft wohl nicht verweigern. Auch ist fraglich, ob durch eine staatlich geführte und finanzierte Stelle überhaupt zu gewährleisten ist, dass der Einzelne – über seinen Tod hinaus – anonym das Internet nutzen kann.

Somit verbleibt der Vorteil, dass die Erben im Vorsorgefall nicht gegenüber jedem einzelnen Dienstanbieter den Todesfall anzeigen müssen. Insofern ist eine staatliche Stelle, die ausreichende Dauerhaftigkeit und Vertrauenswürdigkeit gewährleistet, gegenüber privaten Dienstanbietern zu bevorzugen. Auch ist ein Vorteil, dass die Nutzernamen sämtlicher Dienstanbieter in dem Portal gespeichert sind. Ist der Erblasser jedoch so gewissenhaft und regelt gegenüber jedem Dienstanbieter vertraglich, was mit dem Nutzerkonto nach seinem Tod geschehen soll, ist es wohl daneben möglich, die Nutzernamen der genutzten Online-Dienste für die Erben in einem entsprechenden Dokument privat zu vermerken. Darüber hinaus kann sich zwar grundsätzlich auch der Nachweis von Erbfall, Berechtigung und Identität für die Erben gegenüber den Dienstanbietern als schwierig darstellen, vor allem dann, wenn die Dienstanbieter ihren Sitz im Ausland haben. Existiert jedoch – wie nach diesem Lösungsansatz vorgeschlagen – bereits eine vertragliche Regelung, wäre es effizienter, im Rahmen dieser zusätzlich einheitlich festzulegen, wie die Erben den Eintritt des Vorsorgefalls gegenüber den Dienstanbietern nachweisen können. Diesbezüglich könnte verbraucherfreundlich der Nachweis durch eine Kopie oder einen Scan der Sterbeurkunde vereinbart werden. Vor diesem Hintergrund ist auch zu hinterfragen, ob es ein ausreichendes schutzwürdiges Interesse von Erblassern und Erben gibt, dass allein für den Bereich des digitalen Nachlasses eine staatliche Stelle die Information des Rechtsverkehrs über den Sterbefall übernimmt. Dabei ist zu beachten, dass eine derartige staatliche Fürsorge für den analogen Nachlass nicht stattfindet. In diesem Bereich müssen die Erben gegenüber den jeweiligen Vertragspartnern und Stellen selbst den Erbfall nachweisen, obwohl dort – im Gegensatz zu der Vererbung von Nutzerkonten bei sozialen Netzwerken, wo oft nur ideelle Interessen betroffen sind – häufig (wesentliche) finanzielle Interessen der Erben bestehen. Auch dort kann sich für die Erben der Nachweis als schwierig darstellen, insbesondere wenn der Erblasser ungeordnete Vermögensverhältnisse hinterlassen hat. Der Aufwand des Nachweises des Todesfalls und gegebenenfalls der Erbberechtigung sowie die Schwierigkeiten im Rahmen von Ordnung und Sicherung des Nachlasses sind somit kein spezifisches Problem des digitalen Bereichs, sondern bestehen hinsichtlich des gesamten Nachlasses. Eine derartige Privilegierung des digitalen Nachlasses durch Schaffung eines staatlich geführten und finanzierten Portals gegenüber dem sonstigen Nachlass kann jedoch kaum begründet werden. Aus diesen Gründen kann diesem Lösungsvorschlag nicht gefolgt werden. Ähnliche Wirkungen können auch durch Information der Verbraucher und eine Anregung der Schaffung vertraglicher Regelungen an die Dienstanbieter erreicht werden.

6.5.9.3 Hinterlegung von Vorsorgeurkunde bzw. Masterpasswort in einem zentralen Register

Eine Alternative zu der in Kapitel 6.5.8 auf Seite 217 beschriebenen digitalen Vorsorgeurkunde könnte allerdings die Registrierung der digitalen Vorsorgeurkunden bzw. Masterpasswörter im Zentralen Vor-

sorgeregister oder im Zentralen Testamentsregister darstellen.[224] Auch könnte für die Speicherung der digitalen Vorsorgeurkunden bzw. Masterpasswörter eine eigene Datenbank durch eine vertrauenswürdige und dauerhaft bestehende Organisation geschaffen werden, wobei diese ebenfalls durch die Bundesnotarkammer geführt werden könnte. Diese Institution hat bereits durch das Zentrale Vorsorgeregister und das Zentrale Testamentsregister Erfahrungen mit der Führung entsprechender Register gesammelt.[225] So könnte das Verfahren vereinfacht und zentralisiert werden.[226] Zudem böte dies weitere Sicherheit für die Verbraucher, und im erforderlichen Fall wäre eine zügige Abwicklung möglich,[227] da die erforderlichen Dokumente noch leichter aufgefunden werden könnten.

Gegen eine Hinterlegung der Vorsorgeurkunde bei einer Körperschaft öffentlichen Rechts und damit bei einer zuverlässigen und dauerhaften öffentlichen Institution wie der Bundesnotarkammer sprechen zudem nicht die gleichen Bedenken wie gegen die Hinterlegung bei privaten Dienstanbietern.[228] Auch im Rahmen der Betreuung würde sich die Registrierung in einem derartigen Register eignen, da so der Betreuer bei einer zentralen Stelle Auskunft darüber erlangen kann, ob die betroffene Person die erforderlichen Zugangsdaten hinterlegt hat.

Insbesondere im Zentralen Testamentsregister sind gemäß § 78d I BNotO i. V. m. § 1 ZTRV jedoch nicht die Urkunden selbst oder Angaben zum Inhalt der Urkunde, sondern nur die zum Auffinden der Urkunde erforderlichen Daten registriert. Dadurch soll dem datenschutzrechtlichen Grundsatz der Datensparsamkeit Genüge getan werden, der auch durch die Anforderung einer Erforderlichkeit gemäß § 78c I 2 BNotO besonders festgehalten ist. Die Verwendung der Daten ist auch dadurch eingeschränkt, dass Auskünfte von Amts wegen nur nach dem Tod des Erblassers und nur an das zuständige Nachlassgericht sowie die Verwahrstelle der Urkunde erteilt werden, § 78e S. 3 Nr. 1 und 2 BNotO (Sterbefallmitteilung). Auf Antrag wird nur Gerichten und Notaren Auskunft erteilt, soweit dies im Rahmen ihrer Aufgabenerfüllung erforderlich ist, § 78f I BNotO. Dies sind diejenigen Stellen, deren typische Aufgabe es ist, erbrechtliche Angelegenheiten abzuwickeln, und die einer staatlichen Aufsicht unterliegen.[229] Einen Auskunftsanspruch hat daneben auch grundsätzlich die Person, die von der Datenerhebung betroffen ist. Da das Zentrale Testamentsregister ein nicht-öffentliches Register ist, kann die Auskunft nur erfolgen, wenn hierfür eine gesetzliche Grundlage besteht.[230]
Gleiches gilt für das Zentrale Vorsorgeregister.[231] Auch im Zentralen Vorsorgeregister wird nicht die Urkunde selbst hinterlegt, sondern nur Daten über Existenz und Aufbewahrungsort einer Urkunde sowie typisierte Angaben darüber, welchen Inhalt die Vollmacht hat (insbesondere die Angabe, ob von der Vollmacht Vermögensangelegenheiten und/oder persönliche Angelegenheiten umfasst sind, § 78a III BNotO i. V. m. § 1 I Nr. 5 VRegV).[232]

Hinsichtlich einer Registrierung von Vorsorgeurkunden würde der vorliegende Vorschlag beinhalten,

[224] *Raude*, RNotZ 2017, S. 17 (25).
[225] *G. Müller*, in: Müller/Renner (Hrsg.), Betreuungsrecht und Vorsorgeverfügungen in der Praxis, Rn. 1090; *Bock*, in: Groll/-Steiner (Hrsg.), Praxis-Handbuch Erbrechtsberatung, Rz. 20.197.
[226] *Salomon*, NotBZ 2016, S. 324 (331).
[227] *Raude*, RNotZ 2017, S. 17 (25).
[228] Vgl. hierzu ausführlich Kapitel 6.5.6 auf Seite 209.
[229] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78c Rn. 9.
[230] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78c Rn. 1.
[231] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78b Rn. 2.
[232] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78a Rn. 4.

dass nicht lediglich Angaben über die Person des Erblassers sowie über den Verwahrort von letztwilligen Verfügungen gespeichert werden, sondern auch von Vorsorgeurkunden. Es könnte zwar angedacht werden, einen Scan oder eine (elektronische) beglaubigte Abschrift der Vorsorgeurkunde selbst in dem Register zu speichern. Ausreichend ist es aber wohl auch hinsichtlich der Vorsorgeurkunden, wenn lediglich Angaben über die Person sowie über den Verwahrort der Urkunde gespeichert werden. Allerdings müsste diese Registrierung der Vorsorgeurkunde in das Gesetz aufgenommen werden, da es sich nicht um eine „erbfolgerelevante Urkunde" i. S. d. § 78d I 1 Nr. 1, II BNotO handelt. Die Vorsorgeurkunde ist gerade eine vom Testament getrennte Urkunde. Auch beeinflusst die Vorsorgeurkunde nicht unmittelbar die Erbfolge in dem Sinne, dass sie abstrakt geeignet ist, zu einer Verschiebung der Erbquoten zu führen,[233] sodass die Registrierung nach derzeitiger Rechtslage nicht vorgesehen ist. Die Vorsorgeurkunden müssten somit in den Katalog des § 78d I BNotO aufgenommen werden.

Dies hätte zur Folge, dass auf eine Benachrichtigung der verwahrenden Stelle durch die Registerbehörde gemäß § 78e S. 3 Nr. 2 BNotO i. V. m. § 7 I ZTRV hin die Verwahrstelle nicht nur die erbrechtsrelevanten Urkunden, sondern auch die Vorsorgeurkunde an das zuständige Nachlassgericht weiterleiten könnte. Die Vorsorgeurkunde könnte so im Testamentseröffnungsverfahren berücksichtigt werden, indem im Eröffnungsbeschluss die Existenz der Urkunde, deren Verwahrort und der Begünstigte vermerkt würde. Zur Einsichtnahme in die Urkunde könnten sich die begünstigten Personen im Anschluss an die verwahrende Stelle wenden.
Zu beachten ist jedoch, dass das Masterpasswort selbst nicht im Eröffnungsbeschluss erscheinen oder im Eröffnungsverfahren verkündet werden sollte, da ansonsten wieder die Gefahr besteht, dass nichtberechtigte Personen vom Inhalt der Urkunde – also insbesondere dem Masterpasswort – Kenntnis erlangen könnten.

Somit wären größere Gesetzesänderungen entbehrlich, insbesondere müsste kein neuer Auskunftsanspruch von begünstigten Personen gegen die Registerbehörde oder ein neues Register geschaffen werden. Steht die Vorsorgeurkunde in Zusammenhang mit einer letztwilligen Verfügung, kann sie in das bestehende Zentrale Testamentsregister integriert werden.

Soll die Vorsorgeurkunde in Ergänzung einer Vorsorgevollmacht errichtet werden, ist nach hier vertretener Ansicht eine Registrierung im Zentralen Vorsorgeregister nicht erforderlich. Einem Vorsorgebevollmächtigten ist in der Regel die Bevollmächtigung bekannt. Zudem steht dem Vollmachtgeber die Möglichkeit zur Verfügung, das Innenverhältnis zwischen ihm und dem Vollmachtnehmer genauer zu regeln. Im Rahmen dieser Regelung kann auch mitgeteilt werden, dass eine Vorsorgeurkunde existiert und wo diese hinterlegt ist. In diesem Fall kann der Verbraucher als Vollmachtgeber den Bevollmächtigten eigenverantwortlich informieren. Dies geht auch mit dem Sinn und Zweck des Vorsorgeregisters einher, dass durch die Registrierung die Betreuungsgerichte von Vorsorgevollmachten und Betreuungsverfügungen erfahren, um unnötige Betreuungen zu verhindern.
In diesem Zusammenhang könnte nur angedacht werden, Vorsorgeurkunden zu registrieren, die im Fall des Eintritts der Handlungsunfähigkeit einem Betreuer zur Verfügung stehen sollen.

Die einzelnen Zugangsdaten würden allerdings wie im Rahmen des Kapitels 6.5.8 auf Seite 217 beschrieben auf einem verschlüsselten lokalen Speichermedium durch den Verbraucher aufbewahrt.

[233] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78d Rn. 13.

6.5.10 Vergleich und Bewertung der genannten Verfahren

6.5.10.1 Aus technischer Sicht

Die folgende Tabelle 6.3 fasst die Verfahren zur Bereitstellung von Zugangsdaten anhand der am Anfang des Kapitels genannten praktischen Kriterien zusammen.

Lösung	Zuverlässigk.	Sicherheit	Datenschutz	Gebrauch	Mehrwert
Daten in Verfügung/Vollmacht	+	+	– –	–	–
Passwort-Vergessen-Fkt.	–	–	o	+	–
Password-Manager	+	+	o	+	++
Dig. Datensafe	+	o	–	+	+
Dig. Nachlassdienst	–	–	– –	+	o
Lokales Archiv & Papier	o	+	++	o	+
Dig. Vorsorgeurkunde	+	++	++	+	–
Zentrale Plattform	++	+	+	++	o

Tabelle 6.3: Eigenschaften von Vorsorgemöglichkeiten

Die Auflistung der Zugangsdaten direkt in letztwilligen Verfügungen oder Vollmachten ermöglicht eine gute Auffindbarkeit und rechtliche Durchsetzbarkeit. Allerdings ist deren Nutzung als alleinige Lösung für die Erben evtl. sehr aufwendig und kostspielig. Zudem ist es schwierig, die Daten aktuell zu halten, der Erblasser hat zu Lebzeiten kaum einen Mehrwert von der Lösung. Auch sind die Online-Dienstanbieter nicht direkt an der Lösung beteiligt. Die Erben müssen daher wie bisher ihre Rechte gegenüber den Dienstanbietern persönlich geltend machen. Außerdem sollten die Zugangsdaten nicht direkt in letztwilligen Verfügungen aufgelistet werden – allenfalls in einem separaten Dokument, damit keine unberechtigten Personen Kenntnis von Zugangsdaten erlangen.

Passwort-Vergessen-Funktionen bieten keine gute Vorsorgemöglichkeit, da die sonstigen Konfigurationseinstellungen und Kontodaten (z. B. die E-Mail-Adresse) des Erblassers in der Regel beibehalten werden und allein auf den Kontoinhaber bezogen sind. Der Dienstanbieter wird nicht über den Sterbefall informiert. Die Erben können sich nicht sicher sein, dass eine Übernahme und nachfolgende aktive Nutzung des Kontos – evtl. mit Änderung weiterer persönlicher Daten wie Name und E-Mail-Adresse – vom Anbieter akzeptiert oder zumindest geduldet wird. Aus technischer Sicht gibt es zudem Sicherheitsbedenken gegen die Lösung.

Passwort-Manager und digitale Datensafes scheinen als Vorsorgemaßnahme besser geeignet, wobei es große Unterschiede zwischen den Produkten gibt. Die meisten dieser Produkte sind Serverlösungen, sodass die Lösungen hinsichtlich Sicherheit, Datenschutz und Verfügbarkeit intransparent sind und stark von den Anbietern abhängen. Bei den Diensten zur Verwaltung von Dokumenten wird es noch deutlicher, dass eine hohe Gebrauchstauglichkeit, Verfügbarkeit und Gruppentauglichkeit in der

Regel mit einer Verminderung von Sicherheit und Datenschutz einhergehen. Evtl. wäre eine Versicherungspflicht für diese Dienste des digitalen Nachlasses sinnvoll, um im Falle einer Insolvenz die Fortführung bzw. Übernahme des Dienstes durch ein anderes Unternehmen und damit die langfristige Zuverlässigkeit zu garantieren.

Digitale Nachlassdienste können für Erblasser und Erben hilfreiche Dienste anbieten, insbesondere wenn diese Dienste von etablierten Institutionen und amtlichen Stellen unterstützt und von führenden Online-Dienstanbietern akzeptiert werden. Allerdings haben die Dienstangebote der letzten Jahre gezeigt, dass die Zuverlässigkeit und Langlebigkeit der Dienste fraglich sind. Auch die Sicherheit der hinterlegten Daten (insbesondere bei der Akkumulation von Zugriffsdaten) kann hinterfragt werden.

Die Vorsorgemaßnahme in Form eines lokalen digitalen Archivs und Papier ist eine pragmatische und von den Dienstanbietern unabhängige Lösung. Hier liegt es allerdings in der Verantwortung der Nutzer, ob sie für die digitale Lösung auch gebrauchstaugliche und langlebige Datenformate vorsehen, und ob eine praktische Übergabe der Archive und Papiere an die Erben gesichert ist. Zudem kann es für den Erblasser zu Lebzeiten mühsam sein, die Daten in elektronischer Form und auch auf Papier über Jahre aktuell zu halten.

Die Lösung der digitalen Vorsorgeurkunden kann eine zuverlässigere und sicherere Lösung darstellen als Passwort-Manager, Datensafes oder lokale Archive. Die Zugangsdaten sind in einer digitalen Vorsorgeurkunde mittels eines besonders geschützten Masterpassworts gesichert, das in der Regel in keinem anderen Kontext genutzt und daher auch nicht aktualisiert werden muss. Allerdings erfordern die Aufbewahrung und Aktualisierung der Zugangsdaten von den Nutzern ähnlich viel Disziplin, ohne dass ihnen die Lösung einen Mehrwert zu Lebzeiten böte.

Eine zentrale, staatlich unterstützte Plattform zur Hinterlegung von Urkunden (Testamente, Vorsorgeurkunden, Sterbeurkunden, Erbscheine) mit den entsprechenden Schnittstellen zu den Systemfunktionen der Online-Dienste würde den Erblassern verbindliche Vorsorgemaßnahmen erleichtern und den Erben die Erbringung von Nachweisen vereinfachen. Allerdings wurde eine solche Plattform bisher nicht realisiert, da viele der damit verbundenen organisatorischen und rechtlichen Fragen noch ungeklärt sind.

Die folgende Tabelle 6.4 gibt einen Überblick über die Vor- und Nachteile der einzelnen Verfahren zur Bereitstellung von Zugangsdaten.

Tabelle 6.4: Vorsorgemöglichkeiten mit ihren Vor- und Nachteilen

Lösung	Vorteile	Nachteile
Zugangsdaten in Verfügungen / Vollmachten	✓ Maßnahme im Rahmen erbrechtlicher Verfügungen	✗ Kein Ersatz für Berechtigung durch Vollmacht oder als Erbe ✗ Aktualisierung umständlich und kostspielig ✗ Risiko, dass Unberechtigte Einsicht bekommen

Fortsetzung auf der nächsten Seite

Tabelle 6.4: Vorsorgemöglichkeiten mit ihren Vor- und Nachteilen (Fortsetzung)

Lösung	Vorteile	Nachteile
Passwort-Vergessen-Funktion	✓ Unkompliziert, sofern Erben Zugriff auf E-Mail-Konto/Smartphone des Erblassers haben	✗ Online-Dienste werden nicht vorab und nicht über Sterbefall informiert, Erben müssen sich selbst darum kümmern ✗ Keine umfassende Vorsorge, kein Hinterlegen von Zugriffsdaten für die Erben ✗ Sicherheit umstritten
	✓ Erben können Konten auflösen oder mit Namen des Erblassers weiterführen	✗ Bei Weiterführung Identitätsmissbrauch möglich
	✓ Erben können alle Daten ändern und Konten in ihrem Namen weiterführen	✗ Von vielen Diensten vermutlich nicht erwünscht
Password-Manager	✓ Zugriffsdaten können leicht aktuell gehalten werden	✗ Online-Dienste werden nicht vorab und nicht über Sterbefall informiert, Erben müssen sich selbst darum kümmern ✗ Sicherheitsrisiko durch Anhäufung von Zugriffsdaten beim Anbieter (Ausnahme: KeePass)
	✓ Mehrwert zu Lebzeiten, benutzungsfreundliche Synchronisierung	✗ Keine umfassende Vorsorge, kein Hinterlegen von Dokumenten und Anweisungen ✗ Keine Übergabemechanismen von Tool und Masterpasswort an die Erben
Digitaler Datensafe	✓ Mehrwert zu Lebzeiten, zentrale Ablage von Dokumenten	✗ Online-Dienste werden nicht vorab und nicht über Sterbefall informiert, Erben müssen sich selbst darum kümmern
	✓ Nachlassplanung (Password-Manager, Anweisungen, Kontaktdaten von Vertrauenspersonen) ✓ Gemeinsame Nutzung zu Lebzeiten möglich	✗ Vorsorge oft vergeblich, da viele Dienste nur kurzlebig ✗ Hinterlegte Infos entsprechen nicht unbedingt den Angaben in Testament/ Vollmacht ✗ Sicherheitsrisiko durch Anhäufung von Zugriffsdaten beim Anbieter

Fortsetzung auf der nächsten Seite

Tabelle 6.4: Vorsorgemöglichkeiten mit ihren Vor- und Nachteilen (Fortsetzung)

Lösung	Vorteile	Nachteile
Digitaler Nachlassdienst	✓ Lösungsangebote auch für den Fall, dass keine Vorsorge getroffen wurde ✓ Know-How zu Durchsetzbarkeit und Willensvollstreckung ✓ Mögliche Kooperation zwischen Online-Diensten und Behörden	✗ Online-Dienste werden nicht vorab informiert ✗ Vorsorge oft vergeblich, da viele Dienste nur kurzlebig ✗ Sicherheitsrisiko, falls Anhäufung von Zugriffsdaten ✗ Hohe Kosten
	✓ Willensvollstreckung auch an Erben vorbei möglich	✗ Hinterlegte Infos entsprechen nicht unbedingt den Angaben in Testament/ Vollmacht
	✓ Erben müssen keine Sterbeurkunden vorlegen	✗ Nur erfolgreich, wenn Online-Dienste und Behörden mit Nachlassdienst kooperieren
Lokales Archiv & Papier	✓ Relativ unkompliziert und unabhängig von den Online-Diensten	✗ Online-Dienste werden nicht vorab und nicht über Sterbefall informiert, Erben müssen sich selbst darum kümmern ✗ Erblasser muss Übergabemechanismus selbst definieren ✗ Hinterlegte Infos entsprechen nicht unbedingt den Angaben in Testament/ Vollmacht ✗ Anfällig für Fehler und Verlust ✗ Zugangsdaten sind schnell veraltet
	✓ Geeignet evtl., wenn Sterbefall vorhersehbar	✗ Erben haben evtl. schon zu Lebzeiten des Erblassers unerwünschten Zugriff
Digitale Vorsorgeurkunde	✓ Von vielen Juristen empfohlen, auch in Verbindung mit KeePass ✓ Masterpasswort und konkrete Anweisungen notariell geschützt	✗ Nutzer für Aufbewahrung lokaler Zugangsdaten verantwortlich ✗ Aufwendig und kostspielig
Zentrale Plattform	✓ Umfassende Lösung mit Einbezug der Online-Dienste und Behörden denkbar ✓ Zuverlässig, da staatlich geführt ✓ Nutzung bestehender zentraler Register denkbar	✗ Digitale Dokumente sind keine Original-Urkunden ✗ Viele technische und organisatorisch-rechtliche Fragen offen ✗ Datenschutzbedenken wegen zentraler Speicherung personenbezogener Daten ✗ Staatlich betriebene Plattform erfordert politischen Konsens

Mittelfristig könnten in Deutschland und anderen Ländern evtl. die Institutionen des Gesundheits-

wesens, Banken und Versicherungen als Treuhänder für die digitale Nachlassplanung (einschließlich Datensafe) auftreten, da der Bestand dieser Institutionen staatlich abgesichert und zumindest in Deutschland auch die Portabilität[234] der Daten gesetzlich geregelt ist.

Langfristig wäre eine Internetplattform für den digitalen Nachlass denkbar. Auf eine solche Plattform müssten Bürger, Notare, Nachlassgerichte, Bestatter und Behörden Zugriff haben, um personenbezogene Dokumente wie Testamente, Vollmachten, Sterbeurkunden und Erbscheine gegenseitig zugänglich zu machen und damit den Bürgern die Vererbung digitaler Konten zu erleichtern. Auch bestehen erhebliche Zweifel, ob eine solche zentrale Speicherung personenbezogener Dokumente den Anforderungen des Datenschutzes genügen könnte. Die Online-Dienstanbieter sollten in jedem Fall darauf vorbereitet sein, ihre Dienste mittels geeigneter Systemfunktionen (wie Löschung, Archivierung und Übergabe der Konten) vererbbar zu machen. In diesem Kontext wäre es gut, wenn die Online-Dienste einheitliche Verfahren zum Nachweis über den Tod des Erblassers und zur Identitätsprüfung der Erben unterstützten, vgl. die Kapitel 7.4 auf Seite 316 und 6.8 auf Seite 262.

6.5.10.2 aus rechtlicher Sicht

Technische Möglichkeiten können geeignet sein, die Übertragung des digitalen Nachlasses bzw. der digitalen Angelegenheiten als begleitende Maßnahme zu erleichtern. Die rechtliche Ermächtigung durch die Einsetzung als Erbe oder durch Bevollmächtigung ist aber stets erforderlich, damit ein rechtmäßiger Zugriff erfolgen kann. Durch die technischen Hilfsmittel kann jedoch die praktische Umsetzung der rechtlichen Vorsorge erleichtert werden.

Grundsätzlich stellen die dargestellten rechtlichen Vorsorgemöglichkeiten nur dann tatsächlich eine Übertragung auf die Begünstigten sicher, wenn einerseits der Bestand des digitalen Nachlasses bzw. der digitalen Angelegenheiten nachvollziehbar dokumentiert ist.[235] Andererseits sollten die Zugangsdaten mitgeteilt werden.

Die Nutzung der Passwort-Vergessen-Funktion kann insofern nicht als Vorsorgemaßnahme empfohlen werden, da sie zwar für den Erblasser bzw. Vollmachtgeber einfach ist, sich aber für die Begünstigten als sehr aufwendig und schwierig darstellen kann. So muss zunächst erforscht werden, welche Online-Dienste der Erblasser benutzt hat.

Daneben kann in der derzeitigen Situation keine Empfehlung hinsichtlich der Inanspruchnahme von kommerziellen Dienstanbietern gegeben werden, da hier die Sicherheit der Daten des Verbrauchers infrage steht und zudem eine sehr große Fluktuation bzw. ein hohes Insolvenzrisiko gegeben ist. Auch wenn der Gebrauch digitaler Nachlassdienste im Einzelfall für die Rechtsnachfolger Vorteile bieten kann, besteht keine staatliche oder einheitlich Kontrolle dahingehend, ob die Dienste vertrauenswürdig, verbraucherfreundlich und zuverlässig sind. Eine dahingehende Prüfung ist dem einzelnen Verbraucher auch in der Regel wohl kaum möglich. Erforderlich wäre somit mindestens, dass der

[234] Portabilität meint in diesem Kontext, dass beim Anbieterwechsel eines Kunden der bisherige Anbieter die Kundendaten zum neuen Anbieter übertragen muss, ohne den Kunden mit dieser Aufgabe zu belasten.

[235] *Raude*, RNotZ 2017, S. 17 (24).

dauerhafte Bestand des Unternehmens sowie die Datensicherheit und gewisse Qualitätsstandards gewährleistet sind.

Auch wenn diese Lösung mit Kosten für den Verbraucher verbunden sein kann und eine gewisse Disziplin erfordert, bietet die digitale Vorsorgeurkunde aus rechtlicher Sicht die meisten Vorteile. Hier ist die Sicherheit der Daten weitgehend gewährleistet, und die Zugangsdaten sind für die Erben bzw. Stellvertreter im Vorsorgefall auffindbar. In diesem Zusammenhang könnte auch angedacht werden, die Zentralen Register der Bundesnotarkammer in dem Sinne zu erweitern, dass dort auch die digitale Vorsorgeurkunde registriert werden kann.

6.6 Nachweis der Berechtigung der Erben und Bevollmächtigten

Im Vorsorgefall muss der Bevollmächtigte gegenüber den Dienstanbietern nachweisen, dass er durch eine Vorsorgevollmacht oder einen Betreuungsbeschluss legitimiert ist, auf die Nutzerkonten zuzugreifen. Genauso müssen die Erben im Erbfall ihre Stellung als Erben legitimieren.

6.6.1 Nachweis der Berechtigung des Nutzers

Zunächst muss jedoch nachgewiesen werden, dass das jeweilige Vertragsverhältnis zum Nachlass gehört bzw. der Vollmachtgeber tatsächlich der Nutzer und Vertragspartner ist, sodass auch der Erbe bzw. Bevollmächtigte berechtigt ist, auf die Daten zuzugreifen.

War der Nutzer mit seinem richtigen Namen registriert, lassen sich sowohl seine Berechtigung als auch die Zugehörigkeit des Vertragsverhältnisses zum Nachlass (direkt aus den Vertragsunterlagen) nachweisen. Schwieriger kann sich der Nachweis aber dann darstellen, wenn der Nutzer bei einer Plattform mit einem Pseudonym angemeldet war und der Dienstanbieter den Nutzer nicht eindeutig der im Erbnachweis bzw. in Vollmachtsurkunde oder Betreuerausweis benannten Person zuordnen kann. Zwar weisen Dienstanbieter häufig darauf hin, dass eine Pflicht besteht, sich mit dem richtigen Namen anzumelden. Allerdings ist es beispielsweise bei Instagram üblich, dass der Nutzername ein Pseudonym oder Kürzel des eigenen Namens ist. Zudem wird die Identität vor allem von Anbietern kostenloser Dienste bei Vertragsschluss nicht überprüft. Für den Vorsorgebevollmächtigten, Betreuer oder die Erben kann der Nachweis ihrer Berechtigung dann schwierig sein.[236] Abhilfe könnte in diesem Fall möglicherweise nur dadurch geschaffen werden, dass die Begünstigten nachweisen können, dass die mit dem Vertragsverhältnis verknüpfte E-Mail-Adresse die des Nutzers war[237] oder durch zusätzliche in dem Account hinterlegte Daten wie Fotos, Geburtstag, Wohnort, Arbeitsplatz etc., die

[236] *Kutscher*, Digitaler Nachlass, S. 146, die den Nachweis dann im Anschluss an *Herzog*, NJW 2013, S. 3745 (3747) als „praktisch unmöglich“ bezeichnet; ähnlich auch *Brisch/Müller-ter Jung*, CR 2013, S. 446 (451); *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 76 f.

[237] Hier ist beispielsweise denkbar, dass zwar das Nutzerkonto unter einem Pseudonym geführt wurde, aber die mit dem Nutzerkonto verknüpfte E-Mail-Adresse den wirklichen Namen des Nutzers enthält.

Identität des Nutzers ermittelt werden kann. Vorgeschlagen wird auch, dass der Nachweis in sonstiger Weise etwa dadurch erfolgen kann, dass E-Mails oder Nachrichten, die über den entsprechenden Account empfangen oder versendet wurden und in den Unterlagen des Nutzers gefunden wurden, dem Dienstanbieter vorgelegt werden, damit dieser so die Zugehörigkeit überprüfen kann.[238] Dies ist natürlich nur möglich, wenn der Nutzer Nachrichten auch lokal abgespeichert hat. Allerdings sind diese Möglichkeiten in der Praxis kaum Erfolg versprechend. Ist dem Dienstanbieter somit der wirkliche Name des Nutzers nicht bekannt, ist auch der Nachweis, dass das Nutzerkonto zum Nachlass gehört, kaum oder gar nicht möglich.

6.6.2 Nachweis der Berechtigung eines Erben oder Bevollmächtigten

Ein Erbe kann nach deutschem Recht seine Rechtsposition als Rechtsnachfolger des Erblassers grundsätzlich durch Vorlage eines Erbscheins oder einer eröffneten letztwilligen Verfügung nachweisen.

Ein Bevollmächtigter kann sich bei Vorliegen einer Vorsorgevollmacht durch Vorlage der Vollmachtsurkunde auch gegenüber Dienstanbietern legitimieren.[239] Auch aus diesem Grund ist bei Erteilung der Vollmacht mindestens die Schriftform einzuhalten.

Ist eine Betreuung angeordnet, so erfolgt der Nachweis der Berechtigung des Betreuers durch Vorlage der Bestellungsurkunde bzw. des sogenannten Betreuerausweises i. S. d. § 290 FamFG. Dieser dient der Legitimation des Betreuers im Rechtsverkehr,[240] sodass in der Regel nicht der umfangreichere Bestellungsbeschluss vorgelegt werden muss.[241]

6.6.2.1 Erbrechtliche Nachweise

Hat der Verbraucher vorgesorgt, kann die Erbberechtigung grundsätzlich durch Vorlage der letztwilligen Verfügung nachgewiesen werden. Die Vorlage eines Erbscheins ist in diesem Fall regelmäßig nicht erforderlich.
Handelt es sich um ein öffentliches Testament, so kann dieses zusammen mit dem Eröffnungsbeschluss – auch in Abschrift – vorgelegt werden, § 2232 BGB i. V. m. § 348 I FamFG.[242] Auch hier kann die Rechtsprechung zur Legitimation gegenüber Banken entsprechend angewendet werden, daher darf nicht generell die Vorlage eines Erbscheins verlangt werden.[243]

Liegt ein handschriftliches Testament gemäß § 2247 BGB vor, kann zwar grundsätzlich die Erbenstellung auch durch dieses in Verbindung mit dem Eröffnungsbeschluss nach § 348 FamFG (i. V. m. § 2248

[238] *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 77
[239] Zur Legitimation durch Vorsorgevollmacht gegenüber einer Bank: *LG Detmold*, NZFam 2015, 335.
[240] *Schmidt-Recla*, in: Rauscher (Hrsg.), Münchener Kommentar zum FamFG, § 290 Rn. 1.
[241] *Dodegge*, in: Dodegge/Roth (Hrsg.), Praxiskommentar Betreuungsrecht, Kap. B Rn. 137.
[242] *Brisch/Müller-ter Jung*, CR 2013, S. 446 (451).
[243] *Herzog*, NJW 2013, S. 3745 (3750); *Hoeren*, NJW 2005, S. 2113 (2115); *Preuß*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1922 Rn. 384.

BGB oder § 2259 BGB) nachgewiesen werden, und es darf nicht generell die Vorlage eines Erbscheins verlangt werden. Jedoch ist hinsichtlich eines handschriftlichen Testaments zu beachten, dass diesem nach der Rechtsprechung nicht dieselbe Beweiswirkung für die Rechtsnachfolge zukommt wie einem öffentlichen Testament. Zwar sind beide Formen des Testaments erbrechtlich gleichwertig. Allerdings macht das Gesetz hinsichtlich der Nachweiswirkung Abstufungen.[244] Zudem sind bei einem eigenhändigen Testament „die Gefahren der Rechtsunkenntnis, unklarer Formulierungen, des Urkundenverlusts, seiner Unterdrückung oder Fälschung höher".[245] Dem eröffneten öffentlichen Testament kommt daher grundsätzlich die stärkere Beweiswirkung zu. Beim eigenhändigen Testament besteht insoweit im Einzelfall die Gefahr, als durch dieses die Erbfolge nicht mit der im Rechtsverkehr erforderlichen Eindeutigkeit nachgewiesen werden kann. Nur bei berechtigten Zweifeln an der Erbenstellung dürfen die Dienstanbieter aber die Vorlage eines Erbscheins verlangen.[246]

Zu beachten ist zudem, dass ein (öffentliches oder eigenhändiges) Testament zum Nachweis nur dann ausreicht, wenn sich aus der Verfügung von Todes wegen mit den Mitteln einfacher erläuternder Auslegung ergibt, wer Erbe ist.[247] Die notwendige Eindeutigkeit fehlt dann, wenn zusätzlich die Person des Erben durch ergänzende Auslegung oder durch Rückgriff auf gesetzliche Auslegungs- oder Ergänzungsregeln ermittelt werden muss. In diesem Fall wäre eine Erforschung von Umständen außerhalb der Urkunde erforderlich, die im allgemeinen Rechtsverkehr nicht möglich ist. Weder können Nachlassakten beigezogen werden oder schwierige Rechts- und Auslegungsfragen durch den Vertragspartner geprüft werden. So ist ein Testament beispielsweise dann nicht als Erbnachweis geeignet, wenn die Erbeinsetzung unter einer Bedingung erfolgt ist.[248]

Ist Testamentsvollstreckung angeordnet, kann sich der Testamentsvollstrecker durch Vorlage des Testamentsvollstreckerzeugnisses i. S. d. § 2368 BGB ausweisen.[249] Dieses ermächtigt den Testamentsvollstrecker in ähnlicher Weise wie der Erbschein den Erben legitimiert,[250] im Rechtsverkehr als Testamentsvollstrecker aufzutreten.[251] Daneben kann der Nachweis der Legitimation des Testamentsvollstreckers aber auch durch eine öffentliche letztwillige Verfügung in Verbindung mit dem Eröffnungsbeschluss sowie einem Beleg über die Amtsannahme gegenüber dem Nachlassgericht nachgewiesen werden.[252] Insoweit ist zu beachten, dass diese Regelungen bisher nicht auf ein handschriftliches Testament ausgeweitet wurden, sondern ausdrücklich ein notarielles Testament erforderlich ist.[253] Diese Regeln wurden zwar für den Grundbuchverkehr entwickelt, können jedoch hier entsprechend angewendet werden, da kein Anlass besteht, für den digitalen Nachlass strengere Regeln aufzustellen als im Grundbuchverkehr.

[244] *BGH*, NJW 2016, 2409 (2410).
[245] *BGH*, NJW 2016, 2409 (2411).
[246] Insgesamt hierzu *BGH*, NJW 2016, 2409 ff.; a. A. noch *Günther*, NJW 2013, S. 3681 (3683), insofern, als Banken „bei der Vorlage eines privatschriftlichen Testaments nahezu immer einen Erbschein verlangen dürfen".
[247] *BayObLG*, DNotZ 1995, 306 (308).
[248] *Litzenburger*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 2232 Rn. 22.
[249] *Brisch/Müller-ter Jung*, CR 2013, S. 446 (451).
[250] *Grziwotz*, in: Rauscher (Hrsg.), Münchener Kommentar zum FamFG, § 354 Rn. 6.
[251] *Werkmüller*, ZEV 2000, S. 305 (307); *Grziwotz*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2368 Rn. 1.
[252] OLG München, ZEV 2016, 439 (440); *OLG Hamm*, FamRZ 2017, 1720; *Grotheer*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 2197 Rn. 131; *Lange*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 2197 Rn. 12.
[253] Dazu OLG München, ZEV 2016, 439 (440).

Hat der Verbraucher nicht vorgesorgt, liegt zwar keine letztwillige Verfügung zum Nachweis vor. Allerdings müssen sich die Erben nach deutschem Recht auch in diesem Fall nicht zwingend mittels eines Erbscheins legitimieren. Zwar stellt ein Erbschein eine rechtssichere Alternative dar, da er eine von einem Nachlassgericht ausgestellte öffentliche Urkunde i. S. d. § 417 ZPO ist, welche die Erbenstellung im Rechtsverkehr nachweist. Trotzdem steht den Erben die Möglichkeit offen, den Nachweis der Erbberechtigung in anderer Form zu erbringen. Für den digitalen Nachlass gelten insoweit keine Sonderregelungen.[254] Dienstanbieter dürfen die Leistung auch nicht aufgrund der nach § 2367 BGB befreienden Wirkung der Leistung an den Erbscheinserben bei Unrichtigkeit des Erbscheins verweigern. Auch der Gedanke des Schuldnerschutzes rechtfertigt keine andere Bewertung. Zu berücksichtigen ist insoweit auch das Interesse der Erben an einer möglichst raschen und kostengünstigen Abwicklung des Nachlasses.[255] Dies gilt auch vor dem Hintergrund, dass der wirtschaftliche Wert einiger Bestandteile des digitalen Nachlasses, wie Verträge mit Streaming-Portalen oder sonstiger Abo-Verträge, häufig außer Verhältnis zu Kosten und Zeitaufwand eines Erbscheinsverfahrens stehen.[256] Gleiches kann darüber hinaus gelten, wenn es sich um rein ideelle Werte (wie z. B. Social-Media-Accounts) handelt – selbst dann, wenn wohl auch ein emotionaler Wert dieser digitalen Inhalte für die Erben bestehen kann.[257]
Der digitale Nachlass kann aber dann einen erheblichen wirtschaftlichen Wert erlangen, wenn wichtige Vertragsbeziehungen über den E-Mail-Account abgewickelt wurden, oder ein Girokonto bei einer Online-Bank existiert. Nichtsdestoweniger ist das Verlangen nach Vorlage eines Erbscheins nur bei erheblichen Zweifeln an der Erbenstellung berechtigt.[258] Insofern stellt sich jedoch das rein praktische Problem, als die Erben in dem Fall, dass der Erblasser nicht vorgesorgt hat, anders als durch einen Erbschein ihre Erbenstellung in der Regel nicht rechtsverbindlich nachweisen können. Auch unter diesem Gesichtspunkt ist es den Verbrauchern dringend anzuraten, Vorsorge für ihren digitalen Nachlass zu treffen.

Als problematisch kann sich jedoch darstellen, dass die entsprechenden Urkunden in der Regel nur ihre Nachweisfunktion entfalten, wenn sie in ausreichender Form vorgelegt werden. Insbesondere wenn Dienstanbieter ihren Sitz im Ausland haben, ist es jedoch mit erheblichem Aufwand verbunden, die Urkunde persönlich im Original vorzulegen. Umgekehrt kann sich der Nachweis durch Vorlage eines reinen Scans oder einer bloßen Kopie als problematisch darstellen, da ein hohes Manipulationsrisiko besteht und diesen ein relativ geringer Beweiswert zukommt. Bisher wurde dieser Nachweis deshalb häufig nicht als ausreichend angesehen. Für den digitalen Bereich soll jedoch diskutiert werden, ob nicht in bestimmten Fallgruppen der Nachweis der Berechtigung mittels einer Kopie oder eines Scans der Original-Urkunde unter Abwägung der widerstreitenden Interessen ausreichend sein kann.

[254] BGH, NJW-RR 2005, 599 (600); BGH, NJW 2013, 3716 (3717); BGH, NJW 2016, 2409 (2410); *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 355; *Leipold*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1922 Rn. 45; *Solmecke/Köbrich/Schmitt*, MMR 2015, S. 291 (294); a.A. wohl noch *Herzog*, NJW 2013, S. 3745 (3750). Eine andere Frage ist, ob die Dienstanbieter in ihren AGB einen strengeren Nachweis der Erbberechtigung verlangen dürfen, vgl. dazu oben.

[255] *Grziwotz*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2365 Rn. 32; *BGH*, NJW 2005, 2779 (2780).

[256] *Solmecke/Köbrich/Schmitt*, MMR 2015, S. 291 (294).

[257] Dieses Problem ist aber dann entschärft, wenn das Erbscheinsverfahren nicht allein aufgrund des digitalen Nachlasses durchgeführt wird oder der Nachlasswert ohnehin gering ist.

[258] *Grziwotz*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2365 Rn. 32; *BGH*, NJW 2005, 2779 (2780).

Hinsichtlich des Erbnachweises ist denkbar, dass – wie gegenüber Banken häufig möglich – beglaubigte Abschriften oder Ausfertigungen erteilt werden, die dann jeweils den Dienstanbietern vorgelegt werden.[259] Genauso können auch die Nachweise über die Befugnisse des Testamentsvollstreckers durch beglaubigte Abschriften[260] oder Ausfertigungen erbracht werden. Immerhin können wohl beliebig viele Abschriften und Ausfertigungen erstellt werden, sodass die Erben ihre Erbenstellung gegenüber mehreren Dienstanbietern gleichzeitig nachweisen können, wenn sie diese auf dem Postweg versenden. Trotzdem ist auch dies für die Verbraucher mit erheblichem Aufwand und Kosten verbunden.

Aufgrund dieser Schwierigkeiten für die Verbraucher soll untersucht werden, ob der Nachweis der Erbberechtigung mittels einer Kopie oder eines Scans der eröffneten letztwilligen Verfügung oder des Erbscheins ausreichend ist.

Auch für den Fall, dass die Vorlage eines Erbscheins erforderlich ist, könnte dies einen Vorteil für die Verbraucher darstellen. Zwar muss hierfür überhaupt ein Erbschein vorliegen und damit ein Erbscheinsverfahren durchgeführt werden. Allerdings sind die Kosten, die auf die Verbraucher zukommen, begrenzt. Die Kosten des Erbscheinsverfahrens richten sich zwar nach dem Wert des Nachlasses im Zeitpunkt des Erbfalls, § 40 I 1 Nr. 2 GNotKG. So kann das Erbscheinsverfahren kostspielig werden, wenn der Wert des Nachlasses hoch ist. In der Regel ist bei einem hohen Nachlasswert aber – unabhängig vom digitalen Nachlass – die Durchführung des Erbscheinsverfahrens notwendig, wenn beispielsweise eine Bank für die Auszahlung von Guthaben des Erblassers die Vorlage des Erbscheins verlangt. Im Rahmen des digitalen Nachlasses kommen dann aber keine zusätzlichen Kosten auf die Erben zu, wenn sie den ohnehin erteilten Erbschein kopieren oder scannen und den Online-Dienstanbietern vorlegen können. Ist einmal das Erbscheinsverfahren nur aufgrund des digitalen Nachlasses durchzuführen, weil beispielsweise kein Vermögen, sondern nur ideelle Werte in Form von Social-Media-Accounts den Nachlass bilden, sind auch die Kosten für das Erbscheinsverfahren gering.[261] Da der erteilte Erbschein im Anschluss mehrfach kopiert oder gescannt werden kann, handelt es sich um einmalige geringe Kosten für die Erben.

Eine Kopie oder ein Scan der jeweiligen Urkunde könnte dann ausreichend sein, wenn eine Abwägung der widerstreitenden Interessen der Beteiligten ergibt, dass den Dienstanbietern dieser Nachweis deshalb ausreichen muss, weil sie dadurch ausreichend in ihren Interessen geschützt sind.[262] Als Abwägungspositionen kommen vorliegend die Interessen der Erben, der Dienstanbieter und des Erblassers in Betracht. Unterschieden werden soll auch grundsätzlich danach, ob mit den Accounts und Vertragsbeziehungen finanzielle Interessen verknüpft sind.

[259] BGH, NJW 2016, 2409 (2411 Rn. 25).

[260] *Grotheer*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 2197 Rn. 131.

[261] In § 40 I 1 Nr. 2 GNotKO ist geregelt, dass der Geschäftswert sich nach dem Wert der Nachlasses im Zeitpunkt des Erbfalls richtet. Nach KV 12210 GNotKO beträgt die Gebühr für die Erteilung eines Erbscheins 1,0. Gemäß Anlage 2 zur GNotKO beträgt die Gebühr nach Tabelle B bei einem Geschäftswert bis 500 Euro somit 15,00 Euro.

[262] Dies gilt natürlich unter der Prämisse, dass nicht vertraglich (beispielsweise in AGB) bereits wirksam der erforderliche Nachweis vereinbart ist.

Vertragsbeziehungen ohne monetären Bezug

Die Erben haben grundsätzlich ein berechtigtes Interesse an einer möglichst raschen und kostengünstigen Abwicklung des Nachlasses.[263] Auch die Eröffnung eines Testaments und dessen Beglaubigung nebst Eröffnungsvermerk oder die Ausfertigung eines Erbscheins verursacht Kosten für die Erben, welche sich dadurch multiplizieren können, dass gegenüber jedem einzelnen Dienstanbieter die Erbberechtigung – möglicherweise sogar im Ausland – nachgewiesen werden muss. Zudem ist es aufwendig, das Testament entweder persönlich bei den Dienstanbietern vorzulegen – wozu möglicherweise im Einzelfall gar keine Möglichkeit eröffnet ist – oder die Urkunde an jeden Dienstanbieter postalisch zu versenden. Es ist darüber hinaus mit einem Risiko für die Erben verbunden, die Urkunde (und sei es nur eine beglaubigte Abschrift) durch die Versendung aus der Hand zu geben. Daher ist es grundsätzlich im Interesse der Erben, die Erbberechtigung auch mittels einer Kopie oder eines Scans der Urkunde nachweisen zu können.

Dem könnte ein Interesse der Dienstanbieter entgegenstehen, sich vor einer Haftung bei Herausgabe an nichtberechtigte Personen zu schützen und deshalb einen möglichst sicheren Erbnachweis verlangen zu können.[264] Handelt es sich um einen Nachlassbestandteil mit finanziellem Wert, droht eine doppelte Inanspruchnahme des Unternehmens. Dies kann aber dann nicht wirksam den Interessen der Erben entgegenstehen, wenn im Rahmen einer doppelten Inanspruchnahme keine (wesentlichen) finanziellen Nachteile für das Unternehmen entstehen und auch sonst keine oder nur eine geringfügige Haftung bei Herausgabe an einen Nichtberechtigten droht. Dies kommt vor allem dann in Betracht, wenn ein privater Social-Media-Account Nachlassgegenstand des Erblassers ist. Hier handelt es sich in der Regel nur um das Teilen und Posten von Inhalten, mit denen keine Vermögensinteressen verknüpft sind. Gibt der Dienstanbieter Zugangsdaten an Nichtberechtigte heraus, muss jedenfalls kein Geldbetrag doppelt ausgezahlt werden.

In Betracht kommt jedoch eine anderweitige Haftung aufgrund der Herausgabe von privaten Daten. Anzudenken ist hier zunächst eine vertragliche Haftung. Eine solche wäre dann denkbar, wenn sich der Dienstanbieter in den Vertragsbedingungen zum Schutz der Daten des Nutzers, also insbesondere zur Nichtherausgabe, über seinen Tod hinaus verpflichtet hat. Ist der Schutz der Daten vertraglich geregelt, können sich die Erben als neuer Vertragspartner darauf berufen. Werden die Daten an einen Nichtberechtigten herausgegeben, könnte ein Anspruch aus § 280 I BGB in Betracht kommen. Die Pflicht, die im Account enthaltenen Daten zu schützen, bestünde dann gegenüber den Erben. Im Einzelfall sind die jeweiligen Vertragsbedingungen heranzuziehen. Facebook beispielsweise regelt in seinen Nutzungsbedingungen in Punkt 4.3 jedoch nur vage, dass sie für eine Verletzung der „wesentlichen“ Pflichten haften. Derartige „wesentliche“ Pflichten werden als Pflichten definiert, „die für die Erfüllung der Vereinbarung erforderlich sind, deren Verletzung den Zweck der Vereinbarung gefährden würde, und auf deren Einhaltung du vertrauen kannst.“[265] Aus dieser allgemeinen Regelung lässt sich jedoch keine abstrakt vom konkreten Sachverhalt definierbare Haftung für eine Herausgabe an einen Nichtberechtigten definieren.

[263] Vgl. hierzu die ständige Rechtsprechung des BGH zum Erbnachweis, zuletzt BGH, NJW 2016, 2409, 2410.
[264] Dies als entgegengesetztes Interesse ebenfalls ständige Rechtsprechung des *BGH*, ebd.
[265] Zu finden unter: https://de-de.facebook.com/legal/terms.

Daneben könnte der Dienstanbieter allgemein nach §§ 280 I, 241 II BGB aufgrund einer Verletzung der vertraglichen Leistungstreuepflicht haften, wenn eine schuldhafte Herausgabe an einen Nichtberechtigten erfolgt. Die Leistungstreuepflicht verpflichtet grundsätzlich dazu, den Vertragszweck und den Leistungserfolg weder zu gefährden noch zu beeinträchtigten. Eine derartige Schadensersatzpflicht droht nach der Rechtsprechung gerade, wenn der Vertragspartner einen zu strengen Nachweis für die Erbberechtigung verlangt und so unnötige Kosten für die Erben verursacht.[266] Andererseits könnte der Vertragszweck durch eine Herausgabe an Nichtberechtigte ebenfalls gefährdet sein. Hier kommt jedoch ein über § 280 BGB ersatzfähiger Schaden wohl nur in Betracht, wenn der Dienstanbieter allgemein vertraglich zum Schutz der Daten des Nutzers verpflichtet ist. Eine über die vertragliche Regelung hinausgehende datenschutzrechtliche Haftung besteht nicht. Das Datenschutzrecht ist mit dem Tod einer Person nicht mehr anwendbar.[267]

Stellt die Herausgabe der persönlichen Daten an Nichtberechtigte eine Verletzung des postmortalen Persönlichkeitsrechts dar, kommt auch eine deliktische Haftung der Dienstanbieter in Betracht. So wurde bereits in der Marlene-Dietrich-Entscheidung des BGH erkannt, dass ein postmortaler Persönlichkeitsschutz nur gewährleistet werden kann, wenn der Erbe in die Rolle des Trägers des Persönlichkeitsrechts treten und gegen eine unbefugte Nutzung vorgehen kann. Gibt der Dienstanbieter die Daten an Nichtberechtigte weiter, besteht das Risiko bzw. die Gefahr, dass der Achtungsanspruch des Erblassers erheblich beeinträchtigt wird. Die Gefahr besteht umso mehr, wenn die Anforderungen an den Nachweis gering gehalten werden (Kopie etc.).

Unabhängig von der Unterscheidung nach finanziellen Gesichtspunkten sollte daher in jedem Fall das Interesse des Erblassers an der Wahrung seiner Persönlichkeitsrechte in die Abwägung einfließen. Im Falle der Vorlage eines erbrechtlichen Nachweisdokuments kommt das postmortale Persönlichkeitsrecht des Erblassers als Abwägungsfaktor in Betracht.[268] Hier gilt, je niedriger die Anforderungen an einen Nachweis (beispielsweise Kopie statt Original) sind, desto höher ist das Fälschungsrisiko. Je höher das Fälschungsrisiko ist, desto höher ist das Risiko, dass Nichtberechtigte an die Daten gelangen und durch eine missbräuchliche Datenverwendung den nach dem Tod fortwirkenden Achtungsanspruch des Erblassers erheblich beeinträchtigen. Allerdings können sich auch (zu) hohe Anforderungen an das Nachweisdokument negativ auf das postmortale Persönlichkeitsrecht des Erblassers auswirken. Dies wäre etwa der Fall, wenn die Löschung von Daten aufgrund eines fehlenden Legitimationsdokuments verzögert wird und der Dienstanbieter die Daten währenddessen weiterverarbeitet und verbreitet. Der Erblasser wird dann eher ein Interesse an einer schnellen Umsetzung seines letzten Willens durch die Erben haben und das Risiko, dass sich Nichtberechtigte durch Fälschungen Zugang zu den Daten verschaffen, in Kauf nehmen. Das Interesse des Erblassers an einer praktikablen und schnellen Umsetzung seines letzten Willens überwiegt insoweit.

[266] So auch BGH, NJW 2016, 2409 (2410).

[267] Selbst wenn das Datenschutzrecht anwendbar wäre, würde den Erben im Rahmen von Art. 82 I DSGVO die Anspruchsberechtigung fehlen.

[268] Das Datenschutzrecht ist in diesen Fällen nicht mehr anwendbar, es gilt lediglich für die Daten von Lebenden. Damit können datenschutzrechtliche Aspekte aufseiten des Erblassers auch nicht in die Abwägung eingeführt werden.

Vertragsverhältnisse mit monetärem Bezug

Ähnliches könnte auch für solche Online-Vertragsverhältnisse gelten, die nur in geringem Maße einen finanziellen Wert haben. So könnten die Interessen der Erben beispielsweise auch dann überwiegen, wenn der Nachlassgegenstand eine Vertragsbeziehung zu einem Online-Bezahldienst (bspw. PayPal) ist, auf dem nur ein Guthaben von wenigen Euro verfügbar ist. Auch in diesem Fall könnten Kosten und Aufwand für die Erben im Gegensatz zu den Gläubigerschutzinteressen unverhältnismäßig hoch sein. Da im Rahmen von Vertragsverhältnissen zu Bezahldiensten aber finanzielle Interessen betroffen sind, droht für den Dienstanbieter auf der anderen Seite grundsätzlich die Gefahr der doppelten Inanspruchnahme oder eine Haftung für Schäden, die den wahren Erben entstehen.

Gibt beispielsweise ein Unternehmen wie PayPal die Zugangsdaten an einen Nichtberechtigten heraus, könnte einerseits das über den persönlichen Account verfügbare Guthaben von diesem abgebucht werden. Darüber hinaus könnten die Nichtberechtigten allerdings über das mit einem PayPal-Konto verknüpfte Bankkonto oder die verknüpfte Kreditkarte weitere Zahlungsaufträge erteilen und somit den Erben weitere Schäden zufügen, für die der Dienstanbieter haftet. Insofern besteht ein schutzwürdiges Interesse des Dienstanbieters, einen stärkeren Erbnachweis als eine Kopie der letztwilligen Verfügung oder des Erbscheins zu verlangen. Dies ist jedoch dann anders zu beurteilen, wenn PayPal den Erben keinen unbeschränkten Zugang zu dem Konto gewähren muss, sondern die Erben lediglich Auszahlung eines (geringfügigen) Guthabens und Kündigung des Kontos verlangen. In diesem Fall sind auch die Haftungsrisiken für den Dienstanbieter gering. Datenschutzrechtliche Regelungen sind zwar auch hier nicht mehr anwendbar. Allerdings ist unabhängig von finanziellen Gesichtspunkten der Schutz des postmortalen Persönlichkeitsrechts des Erblassers zu berücksichtigen. Auch im Rahmen der vorliegenden Abwägung überwiegt das Interesse des Erblassers an der praktikablen und schnellen Umsetzung seines letzten Willens.[269]

Die Gläubigerschutzinteressen müssen aber wohl nur dann hinter den Interessen der Erben an einem einfachen Nachweis zurückstehen, wenn die mit dem Vertrag verknüpften Vermögenswerte als geringfügig einzustufen sind. Gehen die Vermögenswerte und somit insbesondere die Haftung der Dienstanbieter über die Geringfügigkeitsschwelle hinaus, müssen die Interessen der Dienstanbieter stärker berücksichtigt werden, sodass ein stärkerer Nachweis der Erbberechtigung verlangt werden kann. Als Wertgrenze für die Geringfügigkeit könnte ein Betrag von 100 Euro festgelegt werden, da für die Eröffnung einer Verfügung von Todes wegen im Verfahren nach § 348 FamFG gemäß Nr. 12101 KV-GNotKG ebenfalls eine pauschale Gebühr in Höhe von 100 Euro anfällt.

Diese Wertung könnte insgesamt auf Online-Vertragsverhältnisse übertragen werden, wenn die Erben lediglich die Kündigung des Vertragsverhältnisses und gegebenenfalls die Auszahlung von Restguthaben zur Nachlassabwicklung begehren, und der Wert die Geringfügigkeitsgrenze nicht überschreitet.

Fraglich ist aber, wie dies bei Online-Vertragsbeziehungen ist, für die monatliche Gebühren fällig werden, wie beispielsweise Streamingdienste. Hier sprechen keine haftungsrechtlichen Interessen der Dienstanbieter gegen eine Legitimation der Erben durch eine Kopie, sondern eher Gewinninteressen

[269] Siehe dazu bereits oben.

dahingehend, den Vertrag weiter fortzuführen. Die rechtmäßigen Erben haben demgegenüber ein Interesse daran, überflüssige Verträge des Erblassers zu kündigen und so den Nachlass von Verbindlichkeiten zu befreien. Da regelmäßig derartige Online-Abos keine Vertragslaufzeit haben und zudem monatlich kündbar sind, sind die Gewinninteressen der Unternehmen an der monatlich fälligen (geringen) Gebühr gegenüber den Interessen der Erben jedoch als nachrangig einzustufen. Auch in diesem Fall sollten die Erben nach der hier gefundenen Wertung in der Lage sein, sich gegenüber den Anbietern mittels einer Kopie oder eines Scans der letztwilligen Verfügung zu legitimieren.

6.6.2.2 Vorsorgevollmacht

Ein Vorsorgebevollmächtigter kann sich im Rechtsverkehr grundsätzlich durch Vorlage der Vollmachtsurkunde legitimieren. Insbesondere bei Vollmachten ist allerdings fraglich, welche Form für die Vorlage verlangt werden darf, da die Erteilung einer Vollmacht selbst von keiner Form abhängt und grundsätzlich auch mündlich erfolgen kann. Besonders im datenschutzrechtlich sensiblen Bereich der digitalen Angelegenheiten bzw. des digitalen Nachlasses werden jedoch in der Praxis Dienstanbieter allein eine mündliche Vollmacht (nachvollziehbar) nicht akzeptieren. Fraglich ist jedoch, ob der Vertragspartner bei jedem Geschäftsgang die Vorlage der Originalvollmacht verlangen darf.

Der Verbraucher kann dem Vorsorgebevollmächtigten den Nachweis seiner Berechtigung grundsätzlich zunächst dadurch erleichtern, indem er dem Dienstanbieter die Bevollmächtigung nach § 171 I BGB kundgibt. So könnte der Verbraucher dem Dienstanbieter mitteilen, dass er eine bestimmte Person als Vorsorgebevollmächtigten benannt hat und diese für und gegen ihn zu handeln befugt ist. Dazu müsste die Person des Vertreters genau angegeben sein, indem der vollständige Name und Wohnort des Vertreters mitgeteilt wird. Gegenüber dem Dienstanbieter bleibt der Vertreter dann solange bevollmächtigt, bis die Kundgabe der Vollmacht auf demselben Wege widerrufen wird, § 171 II BGB. Hierfür ist allerdings Voraussetzung, dass der Dienstanbieter eine solche Mitteilung akzeptiert und zudem, dass den Verbrauchern eine geeignete Möglichkeit zu dieser Kundgebung eröffnet wird. Die praktische Umsetzung könnte sich daher als schwierig darstellen.

Für den Bankverkehr wird vertreten, dass die Bank ein berechtigtes Interesse daran hat, sich die Vorsorgevollmacht bei jedem einzelnen Geschäftsgang im Original oder Ausfertigung (bei notariell beurkundeter Vollmacht, § 47 BeurkG) vorlegen zu lassen. Dies soll selbst dann gelten, wenn bei der Bank eine eigene Ausfertigung hinterlegt ist. Nur dann sei die Bank aufgrund der in der Regel vorliegenden Widerruflichkeit zu jeder Zeit ausreichend nach § 172 BGB in ihrem guten Glauben geschützt, dass die Vollmacht zum Zeitpunkt des Rechtsgeschäfts noch besteht. Die Vertretungsmacht besteht gemäß § 172 II BGB nämlich so lange, bis die Vollmachtsurkunde dem Vollmachtgeber zurückgegeben oder für kraftlos erklärt wird. Nicht ausreichend sei demgegenüber, wenn lediglich eine – selbst notariell beglaubigte – Kopie, beglaubigte Abschrift oder ein Scan der Vollmacht vorgelegt wird, da insoweit das Risiko bestehe, dass die Vollmacht bereits widerrufen ist und das Original zurückgegeben wurde.[270]

[270] *Günther*, NJW 2013, S. 3681 (3684); ebenso *Diehn/Rebhan*, NJW 2010, S. 326 (329) für die Vertretung gegenüber Ärzten.

Die wohl herrschende Meinung verlangt dagegen die Vorlage der Originalvollmacht oder Ausfertigung[271] nur einmalig, nicht bei jedem Vertretergeschäft.[272] Vorlage bedeutet nach der Definition der Rechtsprechung, dass die Vollmacht der sinnlichen Wahrnehmung des Vertragspartners umittelbar zugänglich gemacht wurde.[273] Es soll bei weiteren von der Vertretungsmacht gedeckten Rechtsgeschäften mit demselben Geschäftspartner ausreichen, wenn der Vertreter sich auf die erste Vorlage der Urkunde bezieht. Dies ergibt sich einerseits daraus, dass bereits in den Motiven zum BGB angenommen wird, dass die einmalige Vorlage und spätere Bezugnahme ausreichend sind.[274] Zudem folgt dies aus der Gleichstellung mit der besonderen Kundgabe i. S. d. § 171 BGB. Auch diese muss nur einmalig erfolgen.[275]

Jedenfalls einmal muss jedoch nach einhelliger Ansicht die Originalvollmacht oder eine notarielle Ausfertigung vorgelegt werden. Dies deshalb, weil Kopien oder andere Ablichtungen unbegrenzt vervielfältigt werden können und daher nicht die erforderliche Authentizität aufweisen.[276] Dies ist jedoch mit erheblichem Aufwand verbunden, insbesondere dann, wenn die Dienstanbieter ihren Sitz im Ausland haben. Nach der Definition der Rechtsprechung reicht für die Vorlage zwar aus, wenn diese auf dem Postweg übersandt wird. Allerdings ist es dem Bevollmächtigten wohl auch hier kaum zumutbar, seine Originalvollmacht aus der Hand zu geben. Eine persönliche Anreise zum Sitz jedes Dienstanbieters wird aber tatsächlich kaum durchführbar sein, vor allem dann, wenn der Vollmachtgeber mit vielen verschiedenen Anbietern Online-Vertragsbeziehungen abgeschlossen hat.

Der Vorteil der notariellen Vorsorgevollmacht ist insoweit, dass von dieser (auch mehrere) Abschriften durch den Notar ausgestellt werden können (§ 51 BeurkG) und sie im Rechtsverkehr daher flexibler ist als das Original.[277]

Für den digitalen Bereich könnte allerdings auch für die Vorsorgevollmacht im Einzelfall der Nachweis der Berechtigung mittels einer Kopie oder eines Scans ausreichen. Zwar kann eine Kopie für den Empfänger nie dieselbe Rechtsscheinwirkung entfalten wie das Original. Allerdings könnte die Vorlage einer Kopie erneut dann ausreichen, wenn keine überwiegenden Interessen der Dienstanbieter dafür sprechen, das Original oder eine notarielle Ausfertigungen als Nachweis verlangen zu können. Daneben sind hier für den Fall der Handlungsunfähigkeit, wenn der Verbraucher also noch als Vertragspartner zur Verfügung steht, dessen Interessen stärker zu berücksichtigen als im Erbfall. Darüber hinaus sind die Interessen des Bevollmächtigten in die Abwägung mit einzubeziehen. Es erfolgt erneut eine Differenzierung danach, ob dem Vertragsverhältnis finanzielle Interessen zugrunde liegen.

[271] BGH, NJW 1980, 698 (699); BGH, NJW-RR 2007, 1199 (1201).
[272] *Schilken*, in: J. von Staudinger (Hrsg.), Staudinger BGB § 172 Rn. 4 f.; *Maier-Reimer*, in: Westermann u. a. (Hrsg.), Erman BGB Handkommentar, § 172 Rn. 6 f.; *Schäfer*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 172 Rn. 8.
[273] BGH, NJW 1980, 698 (699); BGH, NJW-RR 2007, 1199 (1201).
[274] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 172 Rn. 22; *Schilken*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 172 Rn. 5; *Mugdan*, Mot. I 239 a. E.
[275] *Schäfer*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 172 Rn. 8; *Schilken*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 172 Rn. 5.
[276] *Schubert* in: Säcker u. a. (Hrsg.), MükoBGB, § 172 Rn. 21.
[277] *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 47 Rn. 4; angedeutet auch bei *Gloser*, MittBayNot 2016, S. 101 (106).

Vertragsverhältnisse ohne monetären Bezug

Der Bevollmächtigte hat grundsätzlich ein Interesse daran, seine Bevollmächtigung möglichst einfach und kostengünstig nachzuweisen, um so im Rechtsverkehr für den Vollmachtgeber handeln zu können. Die Vorlage des Originals der Vollmachtsurkunde gestaltet sich insbesondere im internationalen Rechtsverkehr als aufwendig, insbesondere wenn der Bevollmächtigte den Nachweis gegenüber mehreren Dienstanbietern, die ihren Geschäftssitz im Ausland haben, erbringen muss. Eine Versendung der Vollmachtsurkunde mit der Post ist zwar möglich, aber es ist dem Bevollmächtigten kaum zumutbar, das Originaldokument aus der Hand zu geben. Es wäre daher grundsätzlich im Interesse des Bevollmächtigten, seine Berechtigung mittels einer Kopie oder eines Scans der Vollmachtsurkunde nachweisen zu können.

Hier sind daneben aber besonders die Interessen des Vollmachtgebers in den Mittelpunkt zu stellen. Dessen Interessen gehen einerseits dahin, dass die von ihm erteilte Vollmacht im Rechtsverkehr möglichst umfassend und auf einfachem Wege akzeptiert wird, damit im Fall seiner Handlungsunfähigkeit der Bevollmächtigte möglichst rasch und unkompliziert im Rechtsverkehr für ihn tätig werden kann. Es kann kaum im Interesse des Vollmachtgebers liegen, wenn durch eine zu aufwendige und schwer zu erbringende Legitimation des Bevollmächtigten die Vollmacht praktisch leer läuft. Andererseits hat der Vollmachtgeber ein Interesse daran, dass nicht unberechtigte Personen Geschäfte für ihn abschließen oder seine privaten Daten einsehen können. Daher muss auch hier das Interesse des Vollmachtgebers an der Wahrung etwaiger Persönlichkeitsrechte in die Abwägung einfließen. Im Unterschied zu oben, ist das Datenschutzrecht anwendbar, das Risiko bezieht sich also auf eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung. Grundsätzlich gilt auch hier, dass je niedriger die Anforderungen an einen Nachweis (Kopie statt Original) sind, desto höher ist auch das Fälschungsrisiko. Je höher das Fälschungsrisiko ist, desto höher ist das Risiko, dass Nichtberechtigte an die Daten gelangen und durch eine missbräuchliche Datenverwendung in das Recht auf informationelle Selbstbestimmung der betroffenen Person eingreifen. Ein derartiger Eingriff wiegt schwerer als etwaige Beeinträchtigungen des postmortalen Persönlichkeitsrechts, insoweit müssen die Anforderungen an das Nachweisdokument angepasst werden. Doch im Ergebnis ist auch hier der Praktikabilität und der Schnelligkeit im Rechtsverkehr der Vorzug zu gewähren. Der Erblasser hat stets (zumindest mutmaßlich) ein Interesse an einer schnellen Besorgung seiner Geschäfte durch den Betreuer oder den Bevollmächtigten.

Indem der Vollmachtgeber dem Bevollmächtigten die Vollmachtsurkunde aushändigt, schafft er zudem selbst ein gewisses Risiko für die Entstehung des Rechtsscheins der Bevollmächtigung. Auch hat es der Verbraucher hier selbst in der Hand, inwieweit er die Bevollmächtigung und somit dem Bevollmächtigten Handlungsbefugnisse erteilt.

Insofern besteht jedoch dann ein ähnliches Interesse des Dienstanbieters, nicht unberechtigten Personen (fahrlässig) Zugriff auf die Nutzerkonten des Verbrauchers zu gewähren. Dies gilt insbesondere dann, wenn der Dienstanbieter dafür haftbar gemacht werden kann. Auch ist die Situation anders als im Erbfall, als nicht – wie im Regelfall – die einmalige Nachlassabwicklung begehrt wird, sondern der Bevollmächtigte über eine gewisse Dauer gegenüber dem Dienstanbieter tätig wird und sich so weitergehende Haftungsrisiken ergeben können. Jedenfalls droht aber in dem Fall, dass Zugang zu

einem Nutzerkonto gewährt wird, mit dem keine finanziellen Interessen des Nutzers verknüpft sind – also insbesondere bei einem Social-Media-Account – wie oben bereits festgestellt wurde, keine Haftung in Form einer doppelten Inanspruchnahme. Unter diesem Gesichtspunkt hat ein Dienstanbieter somit nicht die Entstehung von Schäden zu befürchten. Auch hier könnte sich jedoch eine spezielle vertragliche Haftung ergeben, allerdings nur, wenn sich eine solche aus den Vertragsbedingungen im Einzelfall ergibt.

Darüber hinaus ist auch zu beachten, dass die Dienstanbieter im Fall des Handelns des Vertreters ohne Vertretungsmacht immerhin durch die Haftung des falsus procurator nach § 179 I BGB geschützt sind.

Auch hier könnte jedoch eine Haftung unter datenschutzrechtlichen Gesichtspunkten bestehen bzw. datenschutzrechtliche Interessen entgegenstehen.

Vertragsverhältnisse mit monetärem Bezug

Der Vollmachtnehmer könnte aber auch Zugriff auf Accounts begehren, mit denen finanzielle Interessen des Vollmachtgebers verbunden sind. Handelt es sich um eine Vorsorgevollmacht für den Todesfall, kann grundsätzlich auf die Ausführungen zu den erbrechtlichen Nachweisen verwiesen werden.

Ist die Vollmacht jedoch für den Fall der Handlungsfähigkeit erteilt, stellen sich die Interessen insofern anders dar, als gegebenenfalls Konten bei Bezahldiensten nicht nur gekündigt, sondern durch den Bevollmächtigten weitergenutzt werden sollen. So könnte der Bevollmächtigte beliebig viele Zahlungsanweisungen an den Bezahldienst erteilen und auf diese Weise einen hohen Schaden für den Verbraucher verursachen, für den der Bezahldienst bei Vorliegen der weiteren Voraussetzungen haften müsste. In diesem Fall überwiegen wohl die Haftungs- und Gläubigerschutzinteressen, die Zugangsdaten nicht nach bloßer Vorlage einer Kopie der Urkunde herauszugeben.

Soll jedoch auch hier allein die Kündigung von Online-Dauerschuldverhältnissen bzw. die Auszahlung von (geringfügigen) Restguthaben erfolgen, beispielsweise, weil diese für den Verbraucher nutzlos geworden sind, könnte die Vorlage einer Kopie oder eines Scans erneut ausreichen.

Hier sind Kosten und Aufwand für die Verbraucher den haftungsrechtlichen Interessen der Dienstanbieter gegenüberzustellen. Auch hier gilt jedoch, dass – soweit die Geringfügigkeitsschwelle nicht überschritten ist – die geringen Haftungsrisiken der Dienstanbieter hinter dem Interesse von Bevollmächtigtem und Vollmachtgeber zurückstehen müssen. Zwar ist auch hier aufseiten des Vollmachtgebers – unabhängig von finanziellen Gesichtspunkten – sein Interesse an der Wahrung seines Rechts auf informationelle Selbstbestimmung zu beachten. Allerdings sind auch hier besonders die Praktikabilität und die Schnelligkeit des Rechtsverkehrs zu berücksichtigen.[278] Die geringen Haftungsrisiken stehen somit in keinem Verhältnis zu dem Umstand, dass durch den aufwendigen Nachweis die Bevollmächtigung im Einzelfall in der Praxis leer läuft und so die privatautonome Vorsorge des Verbrauchers für seine Handlungsunfähigkeit ausgehöhlt werden könnte.

[278] Siehe dazu bereits ausführlich oben.

6.6.2.3 Bestellungsurkunde des Betreuers

Betreuer legitimieren sich im Rechtsverkehr – beispielsweise gegenüber Banken – in der Regel durch einmalige Vorlage des Betreuerausweises im Original.[279] Dies könnte entsprechend auch für Online-Dienstanbieter gelten, weil die Geschäftspartner und auch die betroffene Person selbst ein Interesse daran haben, dass einer unbefugten Person die Verfügung über die Nutzerkonten nicht ermöglicht wird. Zu beachten ist jedoch, dass der Betreuerausweis selbst keinerlei materiell-rechtliche Wirkung und vor allem keine Rechtsschutzwirkung im Rechtsverkehr dahingehend entfaltet, dass die Betreuerbestellung wirksam erfolgt ist oder noch fortbesteht. Zudem ist die Bestellungsurkunde keine Vollmachtsurkunde i. S. d. §§ 172 ff. BGB. Die gesetzliche Vertretungsmacht des Betreuers hängt von seiner wirksamen gerichtlichen Bestellung ab und besteht auch dann, wenn sich der Betreuer nicht mittels des Betreuerausweises legitimieren kann.[280] Daher besteht – auch aus haftungsrechtlicher Sicht – kein berechtigtes Interesse daran, die Vorlage des Betreuerausweises vor jeder einzelnen Verfügung zu verlangen. Die einmalige Vorlage ist ausreichend, in der Regel aber auch erforderlich.[281] Das Risiko der nicht (mehr) bestehenden Vertretungsmacht wird hier dem Erklärungsempfänger zugemutet. Bei Vertreterbestellung auf gesetzlicher Grundlage besteht auch kein Recht nach § 174 BGB, die Vollmacht zurückzuweisen.[282]

Zumindest einmal müsste der Betreuer danach also den Betreuerausweis im Original vorlegen, was bei Sitz der Dienstanbieter im Ausland mit erheblichen Problemen verbunden sein kann. So ist die persönliche Anreise zur Vorlage der Originalurkunde wohl weder zumutbar noch praktisch durchführbar. Genauso wenig zumutbar ist es jedoch, den Betreuerausweis im Original aus der Hand zu geben und auf dem Postweg zu den Dienstanbietern zu schicken. Dies auch deshalb, da der Betreuerausweis nicht nur zur Legitimation gegenüber *einem* Dienstanbieter benötigt wird, sondern gegenüber zahlreichen Geschäftspartnern des Betroffenen.

Auch hier ist daher zu untersuchen, ob für den Fall der digitalen Angelegenheiten der Nachweis der Betreuerstellung durch eine Kopie oder einen Scan des Betreuerausweises bzw. des Bestellungsbeschlusses erbracht werden kann. Erneut sind die widerstreitenden Interessen im Rahmen einer Abwägung zu berücksichtigen, und es ist danach zu unterscheiden, ob mit dem jeweiligen Vertragsverhältnis finanzielle Interessen verbunden sind.

Vertragsverhältnisse ohne monetären Bezug

Auch der Betreuer hat grundsätzlich ein Interesse daran, seine Berechtigung möglichst rasch und einfach im Rechtsverkehr nachweisen zu können. Insofern decken sich seine Interessen mit denen eines Vorsorgebevollmächtigten, wie sie in Kapitel 6.6.2.2 auf Seite 239 beschrieben wurden.

Die Interessen der betreuten Person sind aber auch hier besonders zu berücksichtigen und können sich anders darstellen als im Rahmen der privatautonomen Bevollmächtigung. Zunächst besteht auch

[279] So auch *Günther*, NJW 2013, S. 3681 (3684 f.).
[280] *Schmidt-Recla*, in: Rauscher (Hrsg.), Münchener Kommentar zum FamFG, § 290 Rn. 1.
[281] LG Oldenburg, Urt. v. 15.5.2009 – 13 62/09; BGH, FamRZ 2010, 968 f.; *Günther*, NJW 2013, S. 3681 (3685).
[282] BGH, FamRZ 2010, 968 f.

aus Sicht der betroffenen Person grundsätzlich ein Interesse daran, dass im Fall ihrer Handlungsunfähigkeit immerhin noch der Betreuer im Rechtsverkehr für sie tätig werden kann. Andererseits soll nicht unnötig ermöglicht werden, dass eine nichtberechtigte Person Einsicht in private Daten erhält. Hier ist die Interessenlage dahingehend anders als im Fall der Bevollmächtigung, als sich zunächst die betroffene Person nicht selbst privatautonom für eine Vertretung durch eine andere Person entschieden hat, sondern ihr ein gesetzlicher Vertreter durch ein Gericht zur Seite gestellt wurde. Zudem hat – im Regelfall – die betroffene Person den Betreuer nicht selbst ausgewählt, sondern ihr wurde eine durch ein Gericht ausgewählte Person zur Seite gestellt, die sie möglicherweise gar nicht persönlich kennt. Die Bestellung und die Handlungen des Betreuers stellen sich somit als staatlich legitimierter Eingriff in die Handlungsfreiheit des Betroffenen dar. Es könnte daher im Zweifel kein so großes Interesse der betroffenen Person an einem einfachen Nachweis der Betreuerstellung bestehen wie im Rahmen der Vorsorgevollmacht, vor allem aufgrund der Gefahr, dass eine dem Verbraucher völlig unbekannte Person unberechtigt Einsicht in private Daten erhalten könnte. Hier ist insbesondere das Interesse der betroffenen Person an der Wahrung ihres Rechts auf informationelle Selbstbestimmung zu berücksichtigen, die sich ähnlich darstellt wie im Rahmen der Legitimation eines Vorsorgebevollmächtigten.[283]

Andererseits ist jedoch zu berücksichtigen, dass dem Betreuer nur in dem Maße Befugnisse erteilt werden, als dies von einem Gericht für erforderlich erachtet wurde. Insbesondere die Ermächtigung zur Einsicht bzw. Kontrolle privater Social-Media-Accounts im Rahmen der Post- und Fernmeldekontrolle nach § 1896 IV BGB wird von einem Gericht nur dann erteilt, wenn von diesem Kommunikationsmedium Gefahren oder Beeinträchtigungen für die betroffene Person ausgehen. Ist dies nicht der Fall, hat der Betreuer ohnehin keine Befugnis, sich Zugang zu privaten Accounts zu verschaffen.[284] Gerade zur Gefahrenabwehr besteht zum Schutz der betroffenen Person jedoch ein Interesse, dass der Betreuer zuverlässig und schnell Zugang zu den betreffenden Accounts erhält und sich durch das einfache Mittel der Übersendung einer Kopie oder eines Scans des Betreuerausweises gegenüber den Dienstanbietern legitimieren kann.

Zusätzlich sind die Interessen der Dienstanbieter an dem Nachweis der Betreuerstellung mittels des Original-Betreuerausweises zu berücksichtigen, wobei auch hier vor allem der Schutz vor einer Haftung maßgeblich ist. Jedenfalls besteht aber keine Gefahr vor einer doppelten Inanspruchnahme unter finanziellen Gesichtspunkten. Darüber hinaus haftet der Dienstanbieter erneut nur dann, wenn dies vertraglich besonders festgelegt ist oder sich aus datenschutzrechtlichen Gesichtspunkten ergibt.[285]

Vertragsverhältnisse mit monetärem Bezug

Zumeist möchte der Betreuer eher (Rechts-)Handlungen im Rahmen von Online-Vertragsverhältnissen mit finanziellem Bezug vornehmen. So kommt auch hier die Kündigung von Dauerschuldverhältnissen oder das Begehren der Zugangsgewährung zu Bezahldiensten in Betracht.

[283] Insoweit wird auf die Ausführungen in Kapitel 6.6.2.2 auf Seite 239 verwiesen.
[284] Siehe hierzu bereits ausführlich oben in Kapitel 3.3.1.1 auf Seite 59.
[285] Siehe hierzu bereits ausführlicher im Rahmen der Vorsorgevollmacht, vgl. Kapitel 6.6.2.2 auf Seite 239.

Der Betreuer hat ein Interesse daran, seine Berechtigung auf möglichst einfachem Wege nachzuweisen, um insbesondere finanzielle Nachteile für die betroffene Person zu vermeiden. Die Legitimation mit dem Original-Betreuerausweis oder der originalen Bestellungsurkunde vor (zahlreichen) Dienstanbietern mit Sitz im Ausland ist demgegenüber aber mit enormen Aufwand verbunden.[286]

Für die vorliegende Fallgruppe ist allerdings gesondert zu untersuchen, ob der strenge Nachweis der Betreuerstellung aus Sicht der Dienstanbieter aus haftungsrechtlichen Gesichtspunkten gefordert werden kann. Dies wäre dann der Fall, wenn die Legitimation durch den Original-Betreuerausweis hinsichtlich der Haftung für die Dienstanbieter einen Vorteil bietet. Dazu ist die Wirkung dieses Nachweises maßgeblich in Rechnung zu stellen. Nach herrschender Auffassung entsteht durch die Vorlage des Originals des Betreuerausweises jedoch nicht wie im Rahmen der Vorlage einer Vorsorgevollmacht ein Rechtsscheintatbestand nach §§ 172 ff. BGB, da der Betreuerausweis keine Vollmachtsurkunde im Sinne dieser Normen ist. Selbst wenn sich die Dienstanbieter vor jedem Einloggen des Betreuers den Betreuerausweis vorzeigen lassen würden, wären sie nicht durch die Rechtsscheinhaftung nach §§ 172 ff. BGB vor Handlungen eines nicht (mehr) bevollmächtigten Betreuers geschützt. Die Vollmacht des gesetzlichen Vertreters darf auch nicht nach § 174 BGB zurückgewiesen werden. Die Dienstanbieter tragen somit ohnehin das Risiko dafür, dass die gesetzliche Vertretungsmacht des Betreuers – trotz Vorlage des Betreuerausweises – nicht (mehr) besteht. Hinsichtlich ihrer Haftung oder ihrer Regressansprüche ändert sich somit durch die Vorlage des Originaldokuments nichts. Dies gilt auch unabhängig davon, ob die mit dem Vertrag verbundenen Vermögensinteressen geringfügig sind oder nicht. Zwar steigt das gegen den einfachen Nachweis anzuführende Haftungsinteresse der Dienstanbieter proportional zu den mit dem Vertrag verbundenen Vermögensinteressen. Allerdings erhöht sich das entgegenstehende Interesse von Betreuer und betroffener Person, auf einfache Weise auf den Vertrag Zugriff zu erhalten ebenfalls, wenn mit dem Vertrag bedeutende Vermögensinteressen verbunden sind.

Dem könnten allerdings Interessen der betreuten Person entgegenstehen. Erneut besteht hier ein Interesse, dass keine unberechtigte Person Zugriff auf Online-Vertragsbeziehungen erhält und so dem Verbraucher Vermögensschäden entstehen. Da die betroffene Person aber durch die gerichtliche Betreuerbestellung nichts zur Schaffung eines falschen Rechtsscheins beigetragen hat, stehen ihr bei Vorliegen der Voraussetzungen gegebenenfalls Regressansprüche gegen den Betreuer oder den Dienstanbieter zu. Demgegenüber können Vermögensnachteile zudem auch dadurch entstehen, dass dem Betreuer der Nachweis seiner Berechtigung nicht oder erst nach geraumer Zeit gelingt und er deshalb nicht für die betroffene Person gegenüber den Dienstanbietern tätig werden kann. Ist der Betreuer ermächtigt, werden im Regelfall durch einen einfachen Nachweis auch keine sonstigen Nachteile für die betroffene Person entstehen, da der Betreuer allgemein verpflichtet ist, die Angelegenheiten so auszuüben, wie es dem Wohl der betroffenen Person entspricht, § 1901 II BGB.

Somit hat der Betreuer ein berechtigtes Interesse daran, die aufwendige und praktisch kaum durchführbare Legitimation durch Vorlage des Original-Betreuerausweises zu vermeiden. Auch die Interessen der betroffenen Person sprechen eher für eine einfache Legitimation. Demgegenüber hat es für die Dienstanbieter haftungsrechtlich keine Vorteile, den originalen Betreuerausweis als Nachweis

[286] Dazu ähnlich bereits oben.

zu verlangen. Daher überwiegt das Interesse von Betreuer und Verbraucher, die Legitimation durch eine Kopie oder einen Scan des Betreuerausweises vorzunehmen. Dies gilt hier unabhängig von dem Wert der mit dem Vertrag zusammenhängenden Vermögensinteressen. Da der Betreuer ohnehin nur im Rahmen seines Aufgabenkreises tätig wird und aufgrund der bereits genannten Gesichtspunkte kann sich nach hier vertretener Ansicht der Betreuer gegenüber Online-Vertragspartnern stets durch Vorlage einer Kopie des Betreuerausweises legitimieren.

6.6.3 Digitalisierung letztwilliger Verfügungen

Nach geltender Rechtslage sind letztwillige Verfügungen in Papierform zu verfassen. Auch der Nachweis der Erbberechtigung im Rechtsverkehr wird in der Regel durch Vorlage einer physischen Urkunde erbracht. Die Möglichkeit, letztwillige Verfügungen in digitale Form zu fassen, könnte allerdings die Erbringung des Erbnachweises für die Verbraucher noch weiter vereinfachen. Dadurch könnte erreicht werden, dass – auch in den Fällen, wo dies als noch erforderlich anzusehen ist – keine physischen Originalurkunden vor Ort mehr vorgelegt werden müssten, sondern die Urkunden digital an die Dienstanbieter übermittelt werden könnten. Zu untersuchen ist jedoch, ob letztwillige Verfügungen in digitaler Form den erbrechtlichen Formerfordernissen genügen. Dies ist insbesondere für eigenhändige Testamente kritisch zu sehen. Hinsichtlich notarieller Testamente und Abschriften der Urkunden könnte dies jedoch eine Alternative darstellen.

6.6.3.1 Handschriftliche Errichtung und Scan

Zunächst ist klarstellend festzuhalten, dass ein eigenhändiges Testament, das der Erblasser selbst, ohne Unterstützung durch einen Notar, verfassen kann, nach den gesetzlichen Formvorschriften zwingend durch den Erblasser selbst handschriftlich geschrieben und unterschrieben sein muss (§§ 2231 Nr. 2, 2247 I BGB). Dies bedeutet, dass der Erblasser das Testament höchstpersönlich und unmittelbar von Hand in seiner individuellen Handschrift verfassen muss.[287] Nur diese handschriftliche Originalurkunde stellt das formwirksame Testament dar. Wird dieses eingescannt oder sonst vervielfältigt, kann eine solche „Kopie“ lediglich den Beweis dafür liefern, dass einmal ein formwirksames Testament existiert hat.[288] Ein solcher Scan kann das Original somit nicht ersetzen.

6.6.3.2 Digitalisierte Handschrift bei eigenhändigem Testament

Diskutiert wird jedoch auch die Frage, ob es den Formanforderungen des § 2247 I BGB genügt, wenn der letzte Wille auf einem Computer oder Tablet mithilfe eines Eingabestifts – sozusagen digital von Hand – verfasst wurde. Zwar handelt es sich bei einem solchen Eingabestift um eine bloße Eingabehilfe. In Verbindung mit einer entsprechenden Zeichen- oder Handschriftsoftware können diese jedoch zum Schreiben auf dem Touchscreen eines Tablets oder einem sogenannten Digitalisierungs-

[287] *Litzenburger*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 2247 Rn. 10.
[288] *Grziwotz*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 2247 Rn. 22, 29.

oder Grafiktablett verwendet werden.
Daneben besteht die Möglichkeit, ähnlich der Verwendung eines gewöhnlichen Kugelschreibers mithilfe eines sogenannten Smartpens oder Digitalstifts je nach Modell auf normalem oder speziellem Papier zu schreiben. Der von Hand geschriebene Text wird dabei während des Schreibvorgangs mithilfe einer im Stift integrierten Infrarotkamera erfasst und auf dem internen Speicher des Smartpens gespeichert. Im Anschluss werden die gespeicherten Daten per Bluetooth, Wifi oder USB-Schnittstelle auf einen verbundenen Computer übertragen. So kann der handschriftlich verfasste Text in digitaler Form gesichert werden.[289]

Möglichkeit des Verfassens eines Testaments in digitaler Form mit technischen Hilfsmitteln

Nach einer Ansicht wird hinsichtlich der Wirksamkeit zwischen der Errichtung mittels Touchpen[290] und der Errichtung mittels Smartpen unterschieden.

Demnach sei es im Rahmen der Errichtung mittels eines Touchpen grundsätzlich möglich, den Text in der eigenen Handschrift digital anzufertigen und zu speichern, sodass er auch dem Erblasser individuell zugeordnet werden kann. So wäre der Text auch – wie erforderlich – lesbar und dauerhaft vorhanden. Erforderlich wäre aus technischer Sicht nur noch, die Urheberschaft hinreichend sicher grafologisch identifizieren zu können. Dann wären hinsichtlich der handschriftlichen Anfertigung im Grundsatz keine wesentlichen Unterschiede zur Errichtung auf einem Blatt Papier erkennbar. Die erforderliche Unmittelbarkeit der Erklärung könne zudem dann bejaht werden, wenn die verwendete Schreibsoftware ausreichend die Funktionsgenauigkeit und Fälschungssicherheit gewährleiste und dies auch nachprüfbar sei. Dann sei ausgeschlossen, dass die Umwandlung der Schrift in Daten durch Dritte oder Systemfehler manipuliert würde, sodass dieser Vorgang prinzipiell mit der analogen Übertragung der Schreibbewegungen von Tinte auf Papier vergleichbar sei. Es sei auch deshalb keine physisch verkörperte Urkunde erforderlich, sondern lediglich eine eigenhändig ge- und unterschriebene Erklärung, da § 2247 I BGB gegenüber § 126 I BGB lex specialis sei. Daher sei auch die Rechtsprechung zu § 126 I BGB nicht auf die Errichtung eines eigenhändigen Testaments zu übertragen. Auch die §§ 126 III, 126a BGB, der Wortlaut des § 2255 BGB („Vernichtung der Testamentsurkunde“) und die historische Auslegung der Norm seien keine Argumente gegen diese Annahme. Ein Testament könne insbesondere dann in nichtphysischer Form errichtet werden, wenn eine nachträgliche Manipulation weitestgehend ausgeschlossen ist.[291] Zu beachten sei insofern auch, dass die Gefahr des Überschreibens oder der Nachbearbeitung auch bei einem mittels (löschbarer) Tinte oder Bleistift geschriebenen Testament bestehe.[292] So könne ein Ausgleich zwischen Allgemeininteressen der Klarheit über die Erbfolge und dem Erblasserinteresse, seine Testierfreiheit möglichst praktikabel und einfach auszuüben, geschaffen werden.
Allerdings müsste der Gesetzgeber konkrete Vorgaben über die technischen Anforderungen an eine entsprechende Software sowie die Datensicherung und -speicherung durch den Erblasser – mögli-

[289] Vgl. dazu auch *Hergenröder*, ZEV 2018, S. 7.
[290] In der übrigen Literatur häufig als Digitalisierungstablett bezeichnet, vgl. z. B. *Mayer*, in: Soergel (Hrsg.) Kommentar zum BGB, § 2247 Rn. 18; *Voit*, in: Reimann/Bengel/Mayer (Hrsg.), Testament und Erbvertrag, § 2247 Rn. 14.
[291] *Hergenröder*, ZEV 2018, S. 7 (8 f.).
[292] *Grziwotz*, in: Gsell u. a. (Hrsg.), BeckOGK BGB § 2247 Rn. 22.

cherweise in Form einer modifizierten qualifizierten elektronischen Signatur – aufstellen.[293] Andererseits wird infrage gestellt, ob unter Berücksichtigung der Testierfreiheit und der technischen Möglichkeiten die Analogie zur Handschriftlichkeit noch verneint werden könne.[294]

Da die technischen Voraussetzungen bei Verwendung eines Smartpen – durch das Schreiben entsteht zunächst ein analoges geschriebenes Dokument auf Papier, das dann mittels Kamera digitalisiert wird – wesentlich unterschiedlich sind, wird auch die rechtliche Beurteilung gesondert vorgenommen. Der digitalisierte Text sei in diesem Fall letztlich nur eine Vervielfältigung des Originaldokuments und somit eine Kopie, die kein wirksames Testament darstellen könne. Etwas anderes könne nur dann angenommen werden, wenn der Erblasser, wie im Rahmen der Erstellung einer Blaupause, ausdrücklich eine weitere, gleichwertige Urschrift errichten wollte. Sei dies nicht der Fall, könne der Kopie im Prozess nur Beweiswirkung zukommen.[295]

Digitale Errichtung widerspricht Formvorschriften des § 2247 I BGB

Nach wohl herrschender Ansicht widerspricht die digitalisierte Errichtung eines Testaments den Formvorschriften des § 2247 I BGB.

Zwar sei auf diese Weise noch die Handschrift des Erblassers individualisierbar. Allerdings sei es möglich, die handschriftlichen Schriftzüge durch Löschen oder Verschieben von Wörtern nachzubearbeiten. Diese Nachbearbeitung würde jedoch dem Erfordernis der handschriftlichen Errichtung nicht genügen. Einerseits drohe so eine Manipulation oder Verfälschung. Andererseits sei im Rahmen der Nachbearbeitung nicht sichergestellt, dass der Erblasser den Zusammenhang seiner Erklärung noch in ausreichender Weise erfassen könne. Aufgrund der Nachbearbeitungsmöglichkeit sei auch nicht sichergestellt, dass der Erblasser den Text nicht nur als Entwurf betrachte, sodass es im Einzelfall am Testierwillen fehlen könne.[296] Es fehle aufgrund dessen zudem an der Verkörperung der Willenserklärung[297] und es bestehe die Gefahr der Vervielfältigung des Dokuments.[298]

Neuerdings wird jedoch auch hier vertreten, dass der Gesetzgeber diese Form der Errichtung dann zulassen könne, wenn die digital errichteten und zertifizierten Testamente die Identifizierungsfunktion und Fälschungssicherheit wie ein eigenhändig errichtetes Testament ermöglichen können.[299]

Digitale Errichtung widerspricht den Formvorschriften des § 2247 I i. V. m. §§ 126 ff. BGB

Nach anderer Ansicht sei die Frage der Zulässigkeit eines digital errichteten Testaments nicht anhand der Formzwecke des § 2247 I BGB zu entscheiden, sondern anhand der Systematik der Formvorschriften, insbesondere des Zusammenhangs mit §§ 126 ff. BGB. Daher sei ein derart errichtetes Testament stets formnichtig.

[293] *Hergenröder*, ZEV 2018, S. 7 (10).
[294] *Grziwotz*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 2247 Rn. 22.
[295] *Hergenröder*, ZEV 2018, S. 7 (10 f.).
[296] *Voit*, in: Reimann/Bengel/Mayer (Hrsg.), Testament und Erbvertrag, § 2247 BGB Rn. 14.
[297] *Mayer*, in: Soergel (Hrsg.), Kommentar zum BGB, § 2247 Rn. 18.
[298] *Obergfell*, in: Hausmann/Hohloch (Hrsg.), Handbuch des Erbrechts, Kap. 6 Rn. 88.
[299] *Baumann*, in: J. von Staudinger (Hrsg.), Staudinger BGB § 2247 Rn. 35.

Dieser systematische Zusammenhang könne nicht durch einen Vergleich des § 2247 III BGB mit § 126 I BGB infrage gestellt werden. Zwar verlange § 126 I BGB formal insofern mehr als § 2247 III 2 BGB, als bei letzterem keine vollständige Namensunterschrift erforderlich sei. Allerdings sei die damit bezweckte Identifizierungsfunktion im Rahmen des Testierens bereits durch das Erfordernis einer vollständig eigenhändigen Errichtung gewahrt. Daher sei das Fehlen der zwingenden Namensunterschrift für das normative Verhältnis der Normen unerheblich. Bei wertender Betrachtung müsse § 2247 I BGB auch als die strengere Formvorschrift angesehen werden, da dort die Erklärung vollständig eigenhändig zu errichten sei. Zudem hätten § 2247 I BGB und § 126 I BGB denselben Wortlaut. Beide würden Eigenhändigkeit verlangen, weshalb die Vorschriften nicht grundsätzlich unterschiedlich ausgelegt werden dürften. Insbesondere im Rahmen der Beweisfunktion könne § 2247 I BGB nicht großzügiger als § 126 I BGB ausgelegt werden, auch weil der Erblasser im Streitfall nicht mehr als Zeuge dienen könne. Etwas anderes könne sich auch nicht daraus ergeben, dass nur § 126 I BGB eine Urkunde verlange. Der Gesetzgeber sei zur Zeit der Schaffung des § 2247 I BGB davon ausgegangen, dass man Testamente nur urkundlich verfassen könne, weshalb eine solche – auch ohne Erwähnung im Wortlaut – grundsätzlich erforderlich sei. Auch daraus folge eine gleichlaufende Auslegung zu § 126 I BGB. Zudem verlange § 2255 BGB ausdrücklich eine Testamentsurkunde.[300]

Da sich der systematische Zusammenhang nicht allein auf § 126 BGB, sondern zudem auf §§ 126a, 126b BGB beziehe, könnten Testamente nie in digitaler Form errichtet werden. Dies gelte deshalb, da aus „§§ 126 III, 126a, 126b BGB folg[e], dass digitale Dokumente das Erfordernis einer eigenhändigen Namensunterschrift im Sinne des § 126 I BGB nicht erfüllen."[301] Begründet wird dies damit, dass die gesetzliche Systematik streng zwischen schriftlichen und digitalen Dokumenten trennen würde. Durch die Regelung § 126 III BGB sei „impliziert", dass ein digitales Dokument der Schriftform nie genügen könne, da die elektronische Form die Schriftform nicht „erfülle", sondern lediglich „ersetze". Auch aus der Gesetzesbegründung ergebe sich, dass die elektronische Signatur nur statt der eigenhändigen Unterschrift ersatzweise erfolgen könne. Weiterhin könne ein digitales Dokument nur dann ausreichend sein, wenn die Anforderungen des § 126a BGB erfüllt seien. Ein handschriftlich digital verfasstes Dokument könne aber nie Funktionsäquivalenz zwischen § 126 I BGB und § 126a BGB herstellen. Es fehle an dem Erfordernis der Eigenhändigkeit. Zudem wäre stets eine qualifizierte elektronische Signatur erforderlich.[302]

Ein digitales Testament sei darüber hinaus deshalb unmöglich, weil § 126 III BGB die elektronische Form „immerhin noch zulässt", eine entsprechende Regelung im Rahmen des § 2247 BGB aber fehle. „Das verdeutlicht, dass der Gesetzgeber die Digitalisierung der Formvorschriften gezielt auf den Bereich des Geschäftsverkehrs beschränkt hat."[303]

Stellungnahme

Jedenfalls zu widersprechen ist der Ansicht, die § 2247 BGB und §§ 126 ff. BGB gleichsetzt. Dies gilt zunächst unter dem Gesichtspunkt der systematischen Verknüpfung von § 126 BGB und § 2247

[300] *Scholz*, AcP 219 (2019), S. 100 (105 ff.); inhaltsgleich *ders.*, ErbR 2019, S. 617 ff.
[301] *Scholz*, AcP 219 (2019), S. 100 (109).
[302] *Scholz*, AcP 219 (2019), S. 100 (109 f.).
[303] *Scholz*, AcP 219 (2019), S. 100 (110).

BGB.

§ 2247 BGB ist lex specialis gegenüber § 126 BGB. Nach der allgemeinen Gesetzessystematik gilt die erbrechtliche Sondervorschrift vorrangig vor der Norm aus dem Allgemeinen Teil. Zwar gilt beispielsweise § 125 BGB auch für die Formunwirksamkeit von Testamenten.[304] Dies gilt allerdings nur, da das Erbrecht keine eigenständige Vorschrift für die Nichtigkeit von eigenhändigen Testamenten aufgrund der Formunwirksamkeit aufstellt. Die Formerfordernisse für die Errichtung sind jedoch in § 2247 BGB speziell geregelt. Auch verlangen zwar beide Nomen die „Eigenhändigkeit". Daraus lässt sich jedoch kein systematischer Zusammenhang ableiten. Vielmehr ist eine handschriftliche Erklärung immer „eigenhändig" – von der eigenen Hand geschrieben – in Abgrenzung zur maschinenschriftlichen Niederlegung einer Erklärung.

Selbst wenn man dies anders sieht, ergibt sich jedenfalls aus der Systematik des § 126 BGB zu den §§ 126a, b BGB kein Verbot der elektronischen Form. Da das Gesetz festlegt, dass die elektronische Form die Schriftform „ersetzt", werden diese Formen gerade gleichgestellt. Die elektronische Form ist eine Sonderform der Schriftform, es handelt sich um gleichwertige Formvorschriften.[305] Etwas anderes gilt nur, wenn die elektronische Form durch Gesetz ausgeschlossen ist, was insbesondere im Rahmen von verbraucherrelevanten Vorschriften der Fall sein kann.[306] Durch die qualifizierte elektronische Signatur können die Formzwecke der Schriftform gleichwertig erfüllt werden, insbesondere die Identifizierungsfunktion und die Fälschungssicherheit.[307] Somit würde sich sogar – würde man eine Übertragung der Wertungen des § 126 BGB auf § 2247 I BGB annehmen – der umgekehrte Schluss ergeben, dass die elektronische Form (dann unter Einhaltung der qualifizierten elektronischen Signatur, § 126a BGB) möglich sein muss, weil sie zwar in den §§ 2247 BGB nicht ausdrücklich genannt, aber eben auch nicht ausgeschlossen ist.

Ist somit vornehmlich auf die Formzwecke des § 2247 I BGB abzustellen, könnte bei entsprechender Sicherstellung der Fälschungssicherheit und Identifikationsmöglichkeit die Errichtung einer letztwilligen Verfügung „digital von Hand" wohl bejaht werden.

Unabhängig davon allerdings, ob man nun die Wirksamkeit eines in digitaler Form geschriebenen Testaments bejaht oder verneint, ist festzuhalten, dass diese Frage noch in keiner Weise durch die Rechtsprechung geklärt ist, und sich auch in der juristischen Literatur noch keine herrschende Meinung herausgebildet hat. Daher ist es letztlich eine offene Rechtsfrage, ob die Wirksamkeit eines solchen Testaments zu bejahen oder zu verneinen ist. Rechtssicherheit könnte hier im Ergebnis nur durch eine Anpassung des Gesetzes, namentlich des § 2247 BGB (und gegebenenfalls weiterer Vorschriften), erreicht werden.[308] Aus diesen Gründen kann nach dem momentanen Stand das Verfassen eines Testaments mit digitalisierter Handschrift nicht empfohlen werden.

Darüber hinaus entsteht im Rahmen der digitalen Errichtung keine dauerhaft physisch verkörperte Urkunde, sondern nur eine digitale Datei. Eine weitere Frage – die bisher auch durch die Literatur noch

[304] *Hecht*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 125 Rn. 50 f.
[305] *Primaczenko/Frohn*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 126a Rn. 1.
[306] *Primaczenko/Frohn*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 126a Rn. 3.
[307] *Wendtland*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 126 Rn. 11.
[308] Deutlicher noch *Baumann*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 2247 Rn. 34, nach dessen Ansicht allein der Gesetzgeber über die Wirksamkeit derartiger Testamente entscheiden kann.

nicht aufgeworfen wurde – ist daher, ob das wirksame Testament in diesem Fall die gespeicherte Datei an sich darstellt, oder ob dieses nur in der Verknüpfung mit dem Speichermedium (beispielsweise dem Tablet oder PC) zu sehen ist. Wäre letzteres der Fall, würde auch die digitale Form des Testaments den Nachweis nicht erleichtern. Durch Ausdruck der Datei kann jedenfalls kein wirksames Testament entstehen, da es dabei – aufgrund der Vergleichbarkeit mit einer Kopie – an der erforderlichen Unmittelbarkeit fehlt.[309]

Zudem ist zu beachten, dass für den wirksamen Nachweis der Erbberechtigung nicht nur das Testament an sich, sondern zudem grundsätzlich der Eröffnungsbeschluss erforderlich ist,[310] der nicht in digitaler Form vorliegt, sodass der hier notwendige Beweis der Erbberechtigung im Rechtsverkehr allein durch die digitale Errichtung des Testaments nicht erleichtert wäre.

6.6.3.3 Digitalisiertes notarielles Testament

Die Form des § 2247 BGB ist jedoch nicht erforderlich, wenn ein Testament zur Niederschrift eines Notars errichtet wird, vgl. §§ 2231 Nr. 1, 2232 BGB. Daher ist hier die Möglichkeit der Errichtung in digitaler Form gesondert zu untersuchen.
Nach der gesetzlichen Regelung wird ein Testament zur Niederschrift eines Notars errichtet, indem der Erblasser dem Notar seinen letzten Willen erklärt oder ihm eine Schrift mit der Erklärung übergibt, dass diese seinen letzten Willen enthält (§ 2232 S. 1 BGB), wobei die Schrift nicht vom Erblasser geschrieben sein muss (§ 2232 S. 2 Hs. 2 BGB, ggf. i. V. m. § 30 BeurkG). Diese Erklärung wird durch einen Notar im Verfahren nach dem BeurkG beurkundet, wobei eine – in der Regel computerschriftliche – Niederschrift (nach den §§ 8 ff. BeurkG) zu erstellen ist.
Erforderlich ist jedoch auch hier die eigenhändige Unterschrift des Erblassers (nach Vorlesen und Genehmigung) im Beisein des Notars, § 13 I 1 BeurkG, sowie die eigenhändige Unterschrift des Notars, § 13 III 1 BeurkG. Die Unterschrift des Erblassers verfolgt aber weniger Zwecke als die Unterschrift unter einer privatschriftlichen Urkunde, insbesondere unter einem eigenhändigen Testament, weshalb an diese Unterschrift deutlich geringere Anforderungen gestellt werden können. Die für die eigenhändige Errichtung entwickelten Grundsätze können daher nicht unbesehen auf § 13 I 1 BeurkG übertragen werden. Die Identitätsfunktion ist bereits durch die Feststellung des Notars gemäß § 10 BeurkG gewahrt. Zudem sind der Fälschungs- und Übereilungsschutz bereits durch das Beurkundungsverfahren an sich sichergestellt.[311] Erforderlich ist aber jedenfalls die Eigenhändigkeit. Diese soll gewährleisten, dass die Unterschrift vom Willen des Unterzeichnenden bestimmt wird und dieser Wille mit dessen eigenen Körperkräften umgesetzt wird, um die stärkste unverfälschbare persönliche Ausdrucksform zu erreichen.[312] Das Schreibmaterial ist insofern gleichgültig.[313] Zweck der Unterschrift i. S. d. § 13 BeurkG ist daher vorrangig die Autorisierungsfunktion. Durch die Unterschrift wird

[309] so auch *Hergenröder*, ZEV 2018, S. 7 (9); *Baumann*, in: J. von Staudinger (Hrsg.), Staudinger BGB, § 2247 Rn. 33.
[310] Siehe dazu bereits ausführlich oben.
[311] *Sticherling*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2232 Rn. 117; *Seebach/Rachlitz*, in: Müller-Engels u. a. (Hrsg.), BeckOGK BeurkG, § 13 Rn. 125.
[312] *Sticherling*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2232 Rn. 125.
[313] *Sticherling*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2232 Rn. 128.

einerseits die Genehmigung der Urkunde durch die Beteiligten dokumentiert und andererseits, dass ihnen die in der Niederschrift enthaltenen Erklärungen als eigene zugerechnet werden sollen.[314]

Aus technischer Sicht könnte wohl die erforderliche eigenhändige Unterschrift auch in digitaler Form erbracht werden, da Notare bereits über die erforderliche Infrastruktur für die qualifizierte elektronische Signatur verfügen, die in diesem Fall notwendig wäre.

Nach den geltenden Regelungen des BeurkG kann jedoch die Niederschrift über Willenserklärungen nach §§ 6 ff. BeurkG – und damit auch ein öffentliches Testament – nicht originär elektronisch errichtet werden. Eine andere Beurteilung lässt sich nicht mit der geltenden Rechtslage vereinbaren. Um das Beurkundungsverfahren als überwiegend papiergebundenes Verfahren[315] in ein elektronisches Verfahren zu verändern, wäre eine (umfassende) Reform des BeurkG erforderlich.

Nach geltendem Recht scheidet daher die elektronische Errichtung eines öffentlichen Testaments aus.

6.6.3.4 Digitalisierung von Abschriften

Im Rechtsverkehr ist jedoch in der Regel die Vorlage einer Abschrift der letztwilligen Verfügung nebst einer Abschrift des Eröffnungsbeschlusses ausreichend. Derartige Abschriften könnten möglicherweise in elektronischer Form erteilt werden.

Die §§ 39a, 39 BeurkG (i. V. m. §§ 33 BNotO, 2a DONot) erlauben die Anfertigung einer elektronisch beglaubigten Abschrift von einer in Papierform errichteten Niederschrift. Das hierzu erstellte Dokument muss mit einer qualifizierten elektronischen Signatur mit dauerhaft prüfbarem Zertifikat versehen werden, § 39 I 2, 3 BeurkG. Allerdings erteilen Notare derartige Abschriften nur im Rahmen ihrer Zuständigkeit. Grundsätzlich sind sie zwar nach § 20 I BNotO zuständig, Abschriften zu beglaubigen. Somit könnten Notare eine bei ihnen verwahrte letztwillige Verfügung in elektronischer Form beglaubigen. Zum Nachweis der Erbberechtigung im Rechtsverkehr ist jedoch nicht nur das (notarielle oder eigenhändige) Testament – im Original oder in Abschrift – an sich erforderlich, sondern es muss zudem bereits ein gerichtlicher Eröffnungsbeschluss hinsichtlich der letztwilligen Verfügung ergangen sein.[316] In diesem Fall ist jedoch die Geschäftsstelle des verfahrensführenden Familiengerichts gemäß § 13 III 1, 2 FamFG zur Erteilung einer beglaubigten Abschrift von letztwilliger Verfügung und Eröffnungsbeschluss zuständig. Für die Form der Beglaubigung können die §§ 39, 42 BeurkG entsprechend angewendet werden.[317] Insoweit ist auch hier die Unterschrift, ein Siegel und eine Angabe über Ort und Tag der Ausstellung erforderlich.

Hinsichtlich der Beglaubigung einer Abschrift könnte aber zusätzlich § 39a BeurkG entsprechend Anwendung finden, sodass auch bei Zuständigkeit des Urkundsbeamten der Geschäftsstelle die elektronische Errichtung denkbar wäre. Das erstellte Dokument wäre dann mit einer qualifizierten elektronischen Signatur zu versehen. Allerdings ist hierfür erforderlich, dass den Gerichten die erforderliche

[314] *Seebach/Rachlitz*, in: Müller-Engels u. a. (Hrsg.), BeckOGK BeurkG, § 13 Rn. 127.
[315] *Theilig* , in: Müller-Engels (Hrsg.), BeckOGK BeurkG § 39a Rn. 9.
[316] Siehe hierzu bereits ausführlich oben.
[317] *Sterndal*, in: Keidel (Hrsg.), FamFG, § 13 Rn. 62.

Infrastruktur sowie das erforderliche Zertifikat zur Verfügung steht. Dies sollte jedoch der Fall sein, soweit bereits die elektronische Gerichtsakte geführt wird, vgl. § 14 FamFG. Auch andere Vorgänge sind im Rahmen der Führung der elektronischen Gerichtsakte qualifiziert elektronisch zu signieren (vgl. bspw. § 14 III FamFG i. V. m. § 130b ZPO), sodass jedenfalls die technischen und organisatorischen Mittel hierfür gegeben sind. Dies ist auch ab 01.01.2026 verpflichtend, § 14 IVa FamFG, sodass spätestens ab diesem Zeitpunkt beglaubigte Abschriften auch in elektronischer Form erstellt werden können. Zuvor erfolgt die Erteilung einer beglaubigten Abschrift jedoch wohl weiter in Papierform, insbesondere da den Bürgern kein Anspruch darauf zusteht, dass die einzelnen Gerichte allein zur Beglaubigung von Abschriften bereits vorher die erforderliche Infrastruktur zur Verfügung stellen.

Ist jedoch die elektronische Erteilung einer Abschrift möglich, liegt den Erben der Nachweis in digitaler Form vor. In diesem Fall können sie den Nachweis ihrer Erbberechtigung digital an die Online-Dienstanbieter übermitteln.

Falls zusätzlich erforderlich ist, dass die Übermittlung der Dokumente besonders gesichert ist, wäre auch dies aus technischer Sicht grundsätzlich möglich.
Für einen sicheren Transport verwenden Web-Anwendungen standardmäßig HTTPS-Verbindungen (auf Basis von SSL/TLS). Für eine Ende-zu-Ende-Verschlüsselung könnte man die Dokumente in einer verschlüsselten Mail oder als verschlüsselte Anhänge einer unverschlüsselten Mail versenden, was allerdings aufwendiger ist, weil man den öffentlichen Schlüssel des Empfängers benötigt (und viele Provider einen solchen Schlüssel nicht anbieten).
Grundsätzlich sollte die Sicherheit der Dokumente aber nicht darauf beruhen, sie geheim oder unzugreifbar halten zu müssen, sondern auf der Güte der Signaturverfahren und der Geheimhaltung/alleinigen Kontrolle der verwendeten Signaturschlüssel.
Dies könnte durch die gerichtliche Erteilung der Abschriften gewährleistet werden.

Auf diese Weise könnten die zum Nachweis erforderlichen Abläufe digitalisiert und für die Verbraucher vereinfacht werden.

6.6.3.5 Erweiterung des Zentralen Testamentsregisters

Der Nachweis der Erbberechtigung könnte möglicherweise auch dadurch erleichtert werden, dass letztwillige Verfügungen in vollständiger Form in das Zentrale Testamentsregister aufgenommen werden und Dritten im Rechtsverkehr bei Glaubhaftmachung eines rechtlichen Interesses Einsicht in das Register zu gewähren ist. Online-Dienstanbieter könnten dann um Einsicht in das Register ersuchen, wenn ein vermeintlicher Erbe Zugang zu einem Nutzeraccount des Erblassers begehrt, um dessen Berechtigung zu überprüfen.

Zwar können in das Register bereits nach derzeitiger Rechtslage sowohl notarielle als auch privatschriftliche Urkunden aufgenommen werden, soweit sich letztere in amtlicher Verwahrung befinden, § 78d III BNotO, da das Register im Allgemeininteresse geführt wird. Insofern kann eine umfassende Registrierung erfolgen und es entsteht keine Diskrepanz dahingehend, dass nur ein Teil der letztwilligen Verfügungen registriert werden kann.

Allerdings entspricht diese Nutzung nicht dem Zweck des Registers, nach dem Tod einer Person zeitnah und ohne Fehler die jeweils aktuelle Verwahrstelle erbrechtsrelevanter Urkunden zu benachrichtigen,[318] damit diese nach dem Tod aufgefunden und Fehler im Eröffnungsverfahren vermieden werden können. Das Zentrale Testamentsregister wird dabei nach einem Todesfall durch das Sterbestandesamt über den Sterbefall informiert und hat die übermittelten Daten mit den registrierten Daten abzugleichen. Bei Feststellung einer Übereinstimmung hat das Zentrale Testamentsregister sowohl das zuständige Nachlassgericht als auch die Verwahrstelle zu informieren, § 78e BNotO. Die Verwahrstelle muss die Daten erhalten, die erforderlich sind, um die Urkunde zu identifizieren und an das Nachlassgericht zu übermitteln. Für diese Aufgaben ist es ausreichend, dass nach § 78d BNotO i. V. m. § 78c II BNotO, § 1 ZtRV lediglich Verwahrangaben zu den erbfolgerelevanten Urkunden in das Register aufgenommen werden. Angaben zum Inhalt der Urkunden werden nicht gespeichert.[319] Hierdurch wird auch dem in § 78c I 2 BNotO festgelegten Grundsatz Rechnung getragen, nach dem die Erhebung und Verwendung der Daten auf das für die Erfüllung der gesetzlichen Aufgaben der Registerbehörde, der Nachlassgerichte und der Verwahrstellen Erforderliche zu beschränken ist (Datensparsamkeit). Insofern müssten insgesamt die Ziele und Aufgaben des Registers zunächst dahingehend verändert werden, dass die registrierten Angaben auch dem Erbnachweis im Rechtsverkehr dienen. Dies ist jedoch mit der momentanen Registerführung nicht zu vereinbaren.

Auch wenn dies erfolgen würde, müsste darüber hinaus ein Auskunftsanspruch von dritten Personen im Gesetz geregelt werden, da es sich bei dem Zentralen Testamentsregister um ein nicht-öffentliches Register handelt. Nach derzeitiger Rechtslage erfolgt eine Auskunft durch die Registerbehörde nur, soweit sie im Rahmen der Aufgabenerfüllung der auskunftsberechtigten Gerichte und Notare erforderlich ist, § 78f I 2 BNotO, außer die Urkunden werden bei ihnen verwahrt, § 78 II BNotO. Dies sind Stellen, deren typische Aufgabe es ist, erbrechtliche Angelegenheiten abzuwickeln, und die einer staatlichen Aufsicht unterliegen.[320] Auch dadurch sind die registrierten Daten besonders vor Missbrauch geschützt. Insofern hat auch nicht die Registerbehörde zu prüfen, ob die Voraussetzungen für die Auskunft vorliegen, sondern die ersuchende Stelle hat dies zu erklären. Das Vorliegen der Voraussetzungen prüft die Registerbehörde nur selbst, wenn sie dazu nach den Umständen des Einzelfalls Anlass hat, § 8 I 1 Nr. 2, 2 ZTRV. Angaben von Privatpersonen über das Vorliegen der Voraussetzungen könnten nicht in dieser Weise vertraut werden, sodass die Registerbehörde verpflichtet wäre, im Rahmen jedes Auskunftsersuchens eine Einzelfallprüfung vorzunehmen. Da es sich bei den registrierten erbfolgerelevanten Urkunden auch nicht – wie beispielsweise im Fall des Sterberegisters – um personenstandsrechtliche Angaben, sondern um privatautonome Verfügungen handelt, müsste ein berechtigtes Interesse der auskunftsersuchenden Person an der Einsicht in das Register besonders begründet werden.

Da zum Nachweis im Rechtsverkehr zudem die Vorlage der letztwilligen Verfügung nicht ausreichend ist, müsste das Register um einen Hinweis ergänzt werden, ob hinsichtlich des betreffenden Testaments bereits ein Eröffnungsvermerk ergangen ist. Zudem kann ein in dem Register gespeichertes Dokument nur unter besonderen Voraussetzungen das Original der Urkunde ersetzen, ohne nur ei-

[318] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78c Rn. 6.
[319] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78d Rn. 5 f.
[320] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, § 78c Rn. 9.

ne Kopie der Urkunde darzustellen. Dies gilt insbesondere für eigenhändige Testamente. Dies wäre nur anders, wenn beispielsweise nach dem Eröffnungsverfahren elektronische, beglaubigte Abschriften der relevanten Urkunden in dem Register gespeichert würden. Allerdings müssten auch hierfür zunächst die rechtlichen Voraussetzungen – insbesondere unter Klärung der Zuständigkeit – geschaffen werden. Jedenfalls ist eine Speicherung der Originalurkunden nicht mit dem Sinn und Zweck des Registers zu vereinbaren. Es müsste wohl ein völlig neues Register mit neuen Voraussetzungen geschaffen werden.
Da jedoch zukünftig elektronisch beglaubigte Abschriften von letztwilliger Verfügung und Eröffnungsbeschluss erteilt werden können und so der Nachweis im Rechtsverkehr bereits vereinfacht erbracht werden kann, ist die Erforderlichkeit der Schaffung eines derartigen Registers nach hier vertretener Ansicht zu verneinen.

6.6.4 Digitalisierung von Vorsorgevollmachten

Auch für Vorsorgevollmachten ist zu untersuchen, ob diese in elektronischer Form erstellt werden können. Für Vorsorgevollmachten gilt nach derzeitiger Rechtslage, dass die Bevollmächtigung durch Vorlage der physischen Originalurkunde oder einer Ausfertigung der notariellen Vollmacht bewiesen werden kann. Wäre die Vorlage einer Vollmacht in digitaler Form, die der verkörperten Vorlage im Original oder in Ausfertigung gleichkommt, möglich, würde dies ebenfalls die Legitimation des Bevollmächtigten im Rechtsverkehr erleichtern. Hierbei ist danach zu unterscheiden, ob die Vollmacht unter Mitwirkung eines Notars erteilt wurde.

6.6.4.1 Digitalisierte Vollmachten in privater Hand

Die Errichtung einer Vorsorgevollmacht unterliegt grundsätzlich keinen Formvorschriften und könnte somit auch mündlich erteilt werden. Daher stehen der Erteilung einer Vorsorgevollmacht in digitaler Form im Ausgangspunkt nicht dieselben Bedenken entgegen wie der Errichtung eines Testaments mittels digitalisierter Handschrift.

Somit ist es grundsätzlich denkbar, eine Vorsorgevollmacht maschinenschriftlich am Computer zu erteilen. Allerdings müsste auch dieses Dokument in einer Art und Weise unterschrieben werden, die der erforderlichen Beweisfunktion genügt. Durch die Signatur müsste jedenfalls bewiesen werden können, dass die Unterschriften von Vollmachtgeber und Vollmachtnehmer stammen, die Erklärung dem Willen der Beteiligten entspricht und zur angegebenen Zeit abgegeben wurde. Letzteres ist insbesondere deshalb erforderlich, um eventuelle Zweifel an der Geschäftsfähigkeit des Vollmachtgebers zum Zeitpunkt der Vollmachterteilung auszuräumen. Zudem ist erforderlich, dass die elektronische Form in gleicher Weise wie die handschriftliche Unterschrift einen Schutz vor nachträglichen Manipulationen und Verfälschungen sicherstellt.

Fraglich ist allerdings, ob hierfür rechtlich die qualifizierte elektronische Signatur i. S. d. §§ 126 III, 126a BGB erforderlich ist, da diese strenge Anforderung im Grundsatz nur für Urkunden gilt, für deren Errichtung das Gesetz die Schriftform vorschreibt. Da diese aber für die Vorsorgevollmacht

gerade nicht erforderlich ist, könnte möglicherweise auch eine elektronische Signatur mit geringeren Anforderungen genügen, die jedoch die notwendige Beweisfunktion erbringt.

Allerdings existiert keine elektronische Signatur, deren Erbringung weniger aufwendig ist, jedoch in gleicher Weise die Beweisfunktionen sicherstellt. Zwar ist eine fortgeschrittene elektronische Signatur mit Zeitstempel technisch vergleichbar mit einer qualifizierten elektronischen Signatur. Bei der fortgeschrittenen elektronischen Signatur wird mithilfe der passenden Software der Vergabestelle die elektronische Signatur mit einem einmaligen Signaturschlüssel erstellt. Somit handelt es sich um ein Softwarezertifikat. Allerdings ist hierfür keine Signaturkarte und kein Kartenlesegerät erforderlich. Nach Art. 26 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 (im Folgenden eIDAS-Verordnung) erfüllt eine fortgeschrittene elektronische Signatur die Anforderungen, dass sie dem Unterzeichner eindeutig zugeordnet werden kann und dessen Identifizierung ermöglicht. Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann, und sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Insoweit sind an diese Unterschrift geringere Anforderungen geknüpft, als an die qualifizierte elektronische Signatur. Beispielsweise ist ein Signaturzertifikat nicht zwingend erforderlich und auch nicht zwingend von einer akkreditierten Zertifizierungsstelle zu erteilen. Zwar kann die Beweisfunktion, dass der Betreffende einen Vorgang zur angegebenen Zeit auslöst, über die Online-Ausweisfunktion erreicht werden. Allerdings bietet dies nur eine Momentaufnahme gegenüber der empfangenden Stelle und besitzt keine bleibende Beweiskraft, die man ohne Weiteres an das Dokument „heften“ könnte. Insoweit ist die fortgeschrittene elektronische Signatur für die Verbraucher zwar einfacher zu erbringen, erfüllt jedoch nicht die gleichen Beweiswirkungen wie die qualifizierte elektronische Signatur. Insbesondere bietet sie nicht dieselbe Fälschungssicherheit (vgl. Anhang II eIDAS-Verordnung).

Um die Wirkungen der handschriftlichen Signatur durch eine elektronische Signatur zu ersetzen, müsste somit aufgrund der erforderlichen Beweiswirkungen die qualifizierte elektronische Signatur erfolgen, obwohl die §§ 126 I, III, 126a BGB eigentlich nicht eingehalten werden müssen. Diese kann jedoch von den Verbrauchern kaum zumutbar von zu Hause aus erbracht werden, da Signaturkarten sehr teuer und in der Handhabung technisch sehr anspruchsvoll sind. Zwar kann ein Signaturzertifikat kostenpflichtig nachträglich von der Bundesdruckerei auf den Personalausweis geladen werden. Allerdings geschieht dies weder automatisch noch verpflichtend, und diese Möglichkeit wird kaum wahrgenommen. Dies ist der Fall, da hierfür von Verbraucherseite kaum Bedarf gesehen wird, und die Handhabung der zusätzlich erforderlichen Signaturkomponenten mit Problemen verbunden ist.

Selbst wenn die qualifizierte elektronische Signatur von Vollmachtgeber und Vollmachtnehmer erbracht wurde, ist die sichere Archivierung der Vollmachtsurkunde durch den einzelnen Verbraucher kaum durchführbar.

Somit ist es technisch derzeit kaum möglich, dass Verbraucher Vorsorgevollmachten privat in elektronischer Form erteilen.

6.6.4.2 Digitalisierte notarielle Vorsorgevollmacht

Wird bei der Errichtung einer Vorsorgevollmacht die notarielle Form gewählt, sind auch hier die Vorschriften des BeurkG zu beachten, insbesondere die eigenhändige Unterschrift durch die Beteiligten, §§ 13 I 1, III BeurkG, also des Vollmachtgebers, des Vollmachtnehmers und des Notars. Auch in diesem Fall ist daher nach den in Kapitel 6.6.3.3 auf Seite 251 gefundenen Ergebnissen auf Grundlage des geltenden BeurkG nicht die originäre Niederschrift der Urkunde in elektronischer Form möglich.

6.6.4.3 Ausfertigungen in elektronischer Form

Allerdings ist erneut denkbar, dass eine Ausfertigung der notariellen Vollmachtsurkunde in elektronischer Form erstellt wird.

Für die Beglaubigung der Abschrift einer notariellen Vollmachtsurkunde gemäß §§ 39, 39a BeurkG besteht zwar die Zuständigkeit von Notaren, sodass hier die elektronische Form möglich wäre. Allerdings genügt die beglaubigte Abschrift einer Vorsorgevollmacht im Rechtsverkehr gerade nicht zur Legitimation des Bevollmächtigten.[321] Vielmehr ist hierfür eine Ausfertigung der Urkunde gemäß der §§ 47 ff. BeurkG erforderlich. Bedeutsam ist hier, dass eine Ausfertigung nur erteilt werden kann, wenn die Urschrift in notarieller Verwahrung verbleibt.[322] Dies ergibt sich auch aus § 48 BeurkG. Die Form der Ausfertigung richtet sich nach § 49 BeurkG. Die Ausfertigung stellt eine mit einem Ausfertigungsvermerk versehene Abschrift der Urschrift dar. Die Abschrift muss mit dem Inhalt der Urschrift übereinstimmen, wobei ausschließlich diese inhaltliche Übereinstimmung, nicht aber eine Übereinstimmung des äußeren Bildes oder die Art der Vervielfältigung bedeutsam ist. Die Abschrift kann daher als Fotokopie, tatsächliche Abschrift oder (erneuter) Ausdruck des Dokuments aus der elektronischen Datenverarbeitung erfolgen. Maßgebliche Aufgabe des Notars im Rahmen der Ausfertigung ist es, die inhaltliche Übereinstimmung der Abschrift mit der Urschrift zu überprüfen.[323] Ab dem 01.01.2022 können (dann nach § 49 I BeurkG n. F.) Ausfertigungen auch in einem Ausdruck der elektronischen Fassung der Urschrift bestehen.
Diese Abschrift ist mit dem Ausfertigungsvermerk zu versehen, der Tag und Ort der Erteilung anzugeben, die Person zu bezeichnen, der die Ausfertigung erteilt wird, und die Übereinstimmung der Ausfertigung mit der Urschrift zu bestätigen. Auch muss sie unterschrieben und mit dem Siegel der erteilenden Stelle versehen werden, § 49 II BeurkG.
Eine dem § 39a BeurkG entsprechende Vorschrift existiert für die Ausfertigung nicht, sodass diese nach geltendem Recht in Papierform erteilt wird.

Technisch wäre es aber wohl möglich, die Ausfertigung in elektronischer Form zu erstellen. Insofern wäre ein Dokument aus der elektronischen Datenverarbeitung des Notars mit dem Ausfertigungsvermerk zu versehen und elektronisch zu unterzeichnen. Lediglich die digitalisierte Handschrift als einfache elektronische Signatur reicht in diesem Fall allerdings nicht aus. Sie ist wie die einfache elektronische Signatur vergleichbar mit einer normalen Mail, in der ein Absender steht, ist beliebig

[321] Vgl. hierzu ausführlich bereits oben; zusätzlich *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 47 Rn. 6.
[322] *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 47 Rn. 14.
[323] *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 49 Rn. 6 f.

kopierbar, fälschbar und hat keine Merkmale, die sich eindeutig einer bestimmten Person zuordnen lassen. Erst die fortgeschrittene elektronische Signatur erfüllt sicherheitstechnische Anforderungen (z. B. Erstellung mit einem geheimen kryptografischen Signaturschlüssel unter der alleinigen Kontrolle des Signierenden).

Besser als eine digitalisierte Handschrift wäre eine biometrische Unterschrift, bei der während des Unterschreibens auf einem speziellen Unterschrift-Pad personenbezogene Merkmale (z. B. Druck, Neigungswinkel des Stifts, Geschwindigkeit usw.) aufgenommen werden. Wie bei jeder Biometrie muss es dazu aber ein sicheres Enrollment geben, bei der sich die Person (auf andere Weise) identifiziert und das biometrische Verfahren ausführt, wobei die Merkmale als Referenzdaten gespeichert werden. Beim eigentlichen Verifikationsverfahren muss die Person dann erneut das biometrische Verfahren ausführen, wobei eine Lebenderkennung (Präsenz der biometrischen Merkmale der Person in diesem Moment) sehr wichtig ist, da aufgenommene biometrische Daten immer auch kopiert werden können. Die Verifikationsdaten werden mit den vorliegenden Referenzdaten verglichen, um zu entscheiden, ob es sich wirklich um die bestimmte Person handelt.

Allerdings können die biometrischen Verifikationsdaten dann nicht einfach einem Dokument hinzugefügt werden, um zu beweisen, dass die Person unterschrieben hat. Denn die aufgenommenen Daten sind leicht kopierbar und obendrein nicht menschenleserlich. Es hängt also von der Sicherheit des Enrollment- und Verifikationsprozesses ab, ob die ausführende Stelle/Anwendung einem Dokument beweiskräftig die Information hinzufügen kann, welche Person unterschrieben hat. Dazu sollte diese Information mit einer qualifizierten elektronischen Signatur versehen werden. Die qualifizierte elektronische Signatur ist als einzige der Handunterschrift gleich gestellt, sodass die Unterschrift auch in diesem Fall in dieser Form erfolgen müsste.

Die Notare verfügen auch bereits über die erforderliche Infrastruktur für eine qualifizierte elektronische Signatur (siehe oben). Durch diese qualifizierte elektronische Signatur können rein digital gespeicherte Dokumente auch ausreichend vor nachträglicher Manipulation oder Verfälschung gesichert werden. Dies ergibt sich auch bereits aus Anhang II der eIDAS-Verordnung, wonach die qualifizierte elektronische Signatur besonders vor nachträglichen Fälschungen schützen soll. Allerdings ist dies nicht für unbegrenzte Zeit möglich, weil die technischen Signaturalgorithmen und verwendeten Schlüssellängen auf längere Zeit gesehen angreifbar werden. Voraussagen für die Sicherheit werden daher maximal für die nächsten 7–10 Jahre gemacht. Vor Ablauf der Algorithmengültigkeit müssten die Dokumente erneut (mit einem verbesserten Verfahren) signiert werden. Das ist zwar aufwendig, aber technisch machbar und automatisierbar.
Insofern ist jedoch zu beachten, dass sich die Ausfertigung nicht bei dem Notar, sondern zur Verwendung im Rechtsverkehr bei dem Vorsorgebevollmächtigten befindet. In der Regel sollte jedoch zum Nachweis der Bevollmächtigung dieser Zeitraum ausreichen. Sollte eine Vorsorgevollmacht einmal länger verwendet werden, so könnte der Verbraucher darauf aufmerksam gemacht werden, dass spätestens nach Ablauf von 10 Jahren die Ausfertigung zu erneuern ist. Die nicht mehr gültige Ausfertigung müsste dann durch den Notar entsprechend gekennzeichnet oder eingezogen werden.

Das erforderliche Siegel des Notars könnte wie im Rahmen von § 39a II BeurkG durch die Bestätigung der Notareigenschaft ersetzt werden. In der Praxis erfolgt dies bereits dadurch, dass auf der Signatur-

karte des Notars neben dessen privaten Signaturschlüssel auch ein sogenanntes berufsbezogenes Attribut, das „Notarattribut“, gespeichert ist.[324] Dadurch wird der Signierende als Notar ausgewiesen. Gemäß § 2a II DONot muss das Notarattribut neben der Notareigenschaft auch den Amtssitz und das Land, in dem das Notaramt ausgeübt wird, sowie die zuständige Notarkammer enthalten. Die Erteilung dieser Bestätigung erfolgt gemäß § 67 III Nr. 5 BNotO durch die Notarkammern.

Allerdings soll die Ausfertigung gerade die Originalurkunde im Rechtsverkehr ersetzen. Insoweit ist nicht lediglich die inhaltliche Übereinstimmung mit der Urschrift, sondern der Besitz der Urkunde maßgeblich.[325] Die Ausfertigung, die der Bevollmächtigte erhält, ersetzt somit den Besitz der Urschrift, die bei dem Notar verbleibt. Insofern wäre es im Rahmen einer elektronischen Erteilung erforderlich, dass die Ausfertigung so kopiergeschützt ist, dass dies entweder gar nicht erfolgen kann oder eine Kopie stets als solche erkennbar ist. Auch müsste im Fall der Rückforderung der Urkunde oder der Beendigung der Bevollmächtigung eine Löschung des Dokuments von den Datenträgern des Bevollmächtigten in der Weise möglich sein, dass dieser das Dokument nicht wiederherstellen kann, um Täuschungen im Rechtsverkehr zu vermeiden.

Für elektronische Ausfertigungen wäre zwar auch denkbar, dass diese nicht direkt an den Bevollmächtigten herausgegeben werden, sondern diese beim Notar verbleiben und der Notar die Ausfertigung an die betreffenden Stellen – beispielsweise die Vertragspartner – übersendet. Allerdings wäre diese Lösung sehr aufwendig, da sich der Bevollmächtigte hierzu für zahlreiche Rechtshandlungen zunächst an den Notar wenden müsste. Eine solche Vorgehensweise wäre mit hohen Kosten und Aufwand für die Verbraucher verbunden und würde auch für die Notare eine weitere Arbeitsbelastung bedeuten.

Soweit diese Voraussetzungen technisch gewährleistet werden können, wäre eine Erteilung von Ausfertigungen in elektronischer Form ebenfalls möglich. Dies würde den Nachweis der Bevollmächtigung im Rechtsverkehr insbesondere gegenüber Vertragspartnern im Ausland für die Verbraucher erleichtern. Hierfür müsste jedoch eine Norm im BeurkG geschaffen werden, die elektronische Ausfertigungen erlaubt und die Voraussetzungen festlegt. Jedenfalls erforderlich ist – ähnlich wie im Rahmen von § 39a BeurkG – die qualifizierte elektronische Signatur durch den Notar und die Bestätigung der Notareigenschaft durch die zuständige Stelle.

6.6.4.4 Erweiterung des Zentralen Vorsorgeregisters

Im Rahmen einer Digitalisierung von Vollmachten könnte auch angedacht werden, die vollständigen Vollmachten in das Zentrale Vorsorgeregister der Bundesnotarkammer aufzunehmen. Allerdings wären hierzu einerseits umfassende Reformen hinsichtlich des – erst kürzlich reformierten – Registers erforderlich. Darüber hinaus lässt sich dies wohl auch nicht mit der dem Register derzeit zugewiesenen Funktion vereinbaren.
Dies ist die Information der mit Betreuungsverfahren befassten Gerichte, die nach Einleitung des Verfahrens das Register abfragen und so von der Existenz von registrierten Verfügungen der betroffenen

[324] *Theilig*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 39a Rn. 22.
[325] *Regler*, in: Müller-Engels (Hrsg.), BeckOGK BeurkG, § 47 Rn. 5.

Person Kenntnis erhalten. Ziel ist es, unnötige Betreuungen zu vermeiden, weshalb die Daten vorrangig dem Sinn und Zweck dienen, über Existenz, Inhalt und Aufbewahrungsort einer Vorsorgevollmacht zu informieren.[326] Somit ist es nicht Sinn und Zweck des Registers, im Rechtsverkehr den Nachweis der Bevollmächtigung zu ermöglichen. Dies könnte das Register in seiner derzeitigen Form auch nicht leisten, da die Vollmachtsurkunden selbst auch deshalb nicht im Zentralen Vorsorgeregister hinterlegt werden, da im Rechtsverkehr immer noch die Vorlage des Originals oder einer Ausfertigung erforderlich ist.[327] Zudem ist die Registrierung unbeachtlich für die Wirksamkeit der Vollmachtserteilung. Sie ist keine öffentliche Bekanntmachung i. S. d. § 171 BGB und schafft keine Rechtsscheintatbestände, sondern dient nur der Erstinformation der Betreuungsgerichte, die zusätzlich die Vollmachtsurkunde in Augenschein nehmen müssen.[328]
Selbst wenn die Urkunden im Register hinterlegt wären, könnte dadurch der erforderliche Beweis nach derzeitiger Rechtslage nicht erbracht werden. Denkbar wäre nur, die typisierten Angaben zum Inhalt der Vollmacht nach § 78a II Nr. 3, III BNotO i. V. m. § 1 I Nr. 5 VRegV um die Angabe zu erweitern, dass die Vollmacht eine Regelung zu den digitalen Angelegenheiten umfasst. Allerdings wäre dann immer noch eine Einsichtnahme in die Vollmachtsurkunde selbst erforderlich.

Zudem wäre auch in diesem Fall zusätzlich erforderlich, dass Dritte im Rechtsverkehr – also beispielsweise Vertragspartner des Vollmachtgebers – einen Auskunftsanspruch hinsichtlich der Registerinformationen erhalten. Nach geltendem Recht besteht ein solcher Auskunftsanspruch nur für Betreuungsgerichte und Landgerichte als Beschwerdegerichte im Betreuungsverfahren, vgl. §§ 78b I 1, 6 VRegV. Unbeschadet bleibt davon das Recht der Betroffenen zur Einsichtnahme in über sie gespeicherte personenbezogene Daten.[329] Ein Auskunftsanspruch von dritten Personen lässt sich jedoch mit der derzeitigen Zielrichtung des Registers nicht vereinbaren. Dies ist insbesondere die Information der Gerichte im Betreuungsverfahren. Eine Auskunft von Dritten im Rechtsverkehr ist damit nicht vereinbar. Ein entsprechender Auskunftsanspruch kann auch nicht aus allgemeinen Erwägungen abgeleitet werden. Da es sich um ein nicht-öffentliches Register handelt, müsste dafür eine gesetzliche Grundlage geschaffen werden.[330]

In diesem Zusammenhang ist auch zu beachten, dass durch § 78h BNotO ein Elektronisches Urkundenarchiv eingeführt wurde, das durch die Bundesnotarkammer geführt werden soll. Ab dem 01.01.2022 sind daher alle neu errichteten (notariellen) Urkunden verpflichtend zu digitalisieren und als „elektronische Fassung der Urschrift“ im Elektronischen Urkundenarchiv zu verwahren.[331] Zwar soll dieses Elektronische Urkundenarchiv so errichtet werden, dass ausschließlich die für die Verwahrung zuständige Stelle Zugang zu diesem hat.[332] Allerdings wird in der Gesetzesbegründung in Aussicht gestellt, „dass das Elektronische Urkundenarchiv aufgrund der dort hinterlegten Strukturdaten in der Zukunft zu einem Vollmachts- und Titelregister weiterentwickelt werden kann. Dies würde dazu führen, dass die Vorlage von Papierausfertigungen von Vollmachten [...] entbehrlich wird [...].“

[326] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 8 § 78a Rn. 1.
[327] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 8 § 78a Rn. 5.
[328] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 8 § 78a Rn. 8.
[329] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 8 § 78b Rn. 2.
[330] *Gutfried*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 8 § 78b Rn. 2.
[331] Vgl. hierzu https://urkundenarchiv.bnotk.de/elektronisches-urkundenarchiv/das-gesetz.
[332] BT-Drucks. 18/10607, S. 39.

So sollen vor allem Banken in die Lage versetzt werden, ihre diesbezüglichen Arbeitsabläufe vollständig zu digitalisieren.[333]
Ein derartiges Register wäre auch im Rahmen des digitalen Nachlasses hilfreich, wenn hinsichtlich des Nachweises der Bevollmächtigung gegenüber Online-Dienstanbietern eine Digitalisierung der Abläufe erfolgen könnte.

6.7 Rechtliche Erforderlichkeit einer Identitätsprüfung der Berechtigten

Der Nachweis, dass ein Erbe oder Bevollmächtigter zu bestimmten Handlungen legitimiert ist, erfolgt im Rechtsverkehr durch Vorlage eines erbrechtlichen Nachweises bzw. der Vollmachtsurkunde respektive des Betreuerausweises. Dadurch ist jedoch noch nicht nachgewiesen, dass die in der Urkunde benannte Person auch diejenige ist, die gegenüber einem Vertragspartner in Erscheinung tritt. Zusätzlich könnte ein Vertragspartner daher auch verlangen, dass ein Identitätsnachweis zu erbringen ist. Grundsätzlich hat der Identitätsnachweis neben der Vorlage der Berechtigungsurkunde aber ergänzende Funktion.

Im analogen Rechtsverkehr ist die Identität eines Berechtigten gegebenenfalls durch Vorlage eines Ausweisdokuments nachzuweisen. Ein Nachweis der Identität kann sich aber dann als schwierig erweisen, wenn der Berechtigte die Berechtigungsurkunde nicht persönlich bei dem Dienstanbieter vorlegt, sondern dies auf postalischem oder digitalem Weg erfolgt. Im digitalen Rechtsverkehr kann sich daher der Identitätsnachweis schwieriger darstellen als bei persönlichem Erscheinen.

Dabei ist fraglich, ob die Dienstanbieter überhaupt die Vorlage eines Ausweisdokuments verlangen können. Dies gilt vor allem dann, wenn im Rahmen der Erstregistrierung keine Identitätsprüfung des Nutzers stattgefunden hat. Der Dienstanbieter müsste dann besondere berechtigte Interessen vorbringen, damit ein (gegebenenfalls aufwendiger) Identitätsnachweis des Rechtsnachfolgers oder Stellvertreters gerechtfertigt werden kann. Insbesondere wenn der Dienstanbieter – beispielsweise im Gegensatz zu einer Bank – gesetzlich nicht zur Identitätsprüfung verpflichtet ist, kommen hier gegebenenfalls nur haftungs- oder datenschutzrechtliche Gesichtspunkte in Betracht, die virulent werden, wenn eine Herausgabe von Daten oder Guthaben an nichtberechtigte Personen erfolgt. Gegebenenfalls kann es für die Dienstanbieter als Identitätsnachweis daher ausreichend sein, wenn der mutmaßliche Erbe oder Bevollmächtigte in Besitz einer (eröffneten) letztwilligen Verfügung oder einer Vollmachtsurkunde ist. Da entsprechende Dokumente jedoch abhanden kommen oder entwendet werden können, und der Berechtigte in der Regel nicht persönlich vor dem Dienstanbieter erscheint, kann in bestimmten Fällen ein Interesse daran bestehen, dass die Identität des Berechtigten gesondert nachgewiesen wird.

Allerdings können die Dienstanbieter dann keinen aufwendigen Identitätsnachweis verlangen, wenn nach der in Kapitel 6.6 auf Seite 231 gefundenen Wertung lediglich eine Kopie des Legitimationsnachweises verlangt werden kann. Die Vereinfachung des Nachweises darf nicht durch eine komplizierte

[333] BT-Drucks. 18/10607, S. 38.

Identitätsprüfung wieder ausgehebelt werden. Insbesondere Social-Media-Dienstanbieter dürfen daher keinen strengen Identitätsnachweis der Begünstigten fordern.

Auch insgesamt muss die Identitätsprüfung für die Verbraucher so ausgestaltet sein, dass sie mit zumutbarem zeitlichen und finanziellen Aufwand erfolgen kann. Dies gilt vor allem vor dem Hintergrund, dass die Dienstanbieter ihren Sitz im Ausland haben und den Erben bzw. Stellvertretern kaum zugemutet werden kann, die erforderlichen Dokumente persönlich vorzulegen.

6.8 Verfahren zur Identitätsprüfung der Berechtigten

Nachdem der Dienstanbieter vom Tod des Erblassers und ggf. von den Namen der Erben Kenntnis erlangt hat, werden die Erben wahrscheinlich auf den geerbten Online-Dienst zugreifen wollen. Dazu sollte eine angemessene Identitätsprüfung stattfinden. Im Folgenden werden Verfahren vorgestellt, mit denen Erben ihre Identität gegenüber den Dienstanbietern nachweisen können. Dabei sollen die Verfahren daraufhin bewertet werden, ob sie sowohl für die Verbraucher (Erben) als auch für die Dienstanbieter geeignet erscheinen. Wichtige Kriterien dafür sind:

- **Qualität**: Handelt es sich um einen starken Identitätsnachweis? Ist die Lösung sicher? Sind die Daten qualitativ hochwertig, d. h. entsprechen sie den Daten in hoheitlichen Ausweisdokumenten?
- **Einfachheit (Nutzer)**: Ist die Lösung gebrauchstauglich und aus Nutzersicht schnell zu realisieren?
- **Kostenlos**: Liegen die für die Lösung notwendigen Komponenten schon jetzt den meisten Nutzern vor?
- **Einfachheit (Anbieter)**: Ist die Lösung aus Sicht der Dienstanbieter leicht zu realisieren?
- **Verbreitung**: Ist die Lösung weit verbreitet und auch zumindest in Europa grenzüberschreitend im Gebrauch?

Grundsätzlich ist fraglich, ob ein Dienst für das Vererben eines Kontos ein stärkeres und eindeutigeres Identifizierungsverfahren benötigt als bei der Erstregistrierung der eigentlichen Kontoinhaber zur Anwendung kommt. International aktive Online-Dienstanbieter wie PayPal fordern bei Bedarf von den Nutzern einfach das Hochladen eingescannter Dokumente an – beispielsweise zur Eröffnung eines Geschäftskontos den eingescannten Personalausweis, Handelsregisterauszug, Kontoauszug oder eine Rechnung –, um die Identität des Unternehmens nachzuweisen, ohne dass dabei ein direktes Online-Identitätsnachweisverfahren zum Einsatz käme.[334, 335]

[334] PayPal: Schritt für Schritt zu Ihrem PayPal-Konto, https://www.paypal.com/de/webapps/mpp/verify.

[335] PayPal: PayPal-Leitfaden für den öffentlichen Sektor, https://hilfe.feripro.de/_static/files/2018-10-19_Leitfaden_Vertragsschluss_PayPal.pdf.

6.8.1 Identifikation persönlich vor Ort beim Anbieter oder mittels Ausweiskopien

6.8.1.1 Technische Darstellung und Bewertung

Grundsätzlich könnten Dienstanbieter als Option vorsehen, dass sich Erben persönlich vorstellen, einen Erbschein vorlegen und sich mit einem gültigen Ausweisdokument (Personalausweis oder Reisepass)[336] ausweisen, schließlich ein entsprechendes Formular ausfüllen und unterschreiben. Eine persönliche Vorstellung ist möglich, für den Verbraucher aber sehr umständlich, vor allem, wenn er sich gegenüber mehreren Anbietern im Ausland legitimieren muss. Ein solcher Identitätsnachweis ist mit einer Legitimationsprüfung vergleichbar wie sie Banken gemäß § 10 GwG bei der Einrichtung eines Bankkontos durchführen. Bei einer Legitimationsprüfung werden Name, Vorname, Geburtstag, Geburtsort, Staatsangehörigkeit und Wohnanschrift anhand eines persönlich vorgelegten Ausweises überprüft. Der Ausweis muss dabei gemäß § 8 II 2 GwG vollständig kopiert oder digital erfasst werden. Bietet der Dienstanbieter seinen Kunden keine öffentlichen Filialen (z. B. im Fall von Internetbanken), dann kann eine aus Sicht des Dienstanbieters unpersönliche Legitimationsprüfung durchgeführt werden. In Deutschland wird in der Regel ein Postident-Verfahren[337] genutzt, siehe Kapitel 6.8.7 auf Seite 276. Aber auch die direkte Nutzung der Online-Ausweisfunktion ist möglich, siehe Kapitel 6.8.8 auf Seite 277.

Die meisten Dienstanbieter und auch Banken, die ihren Sitz außerhalb von Deutschland haben, sehen im Rahmen einer Kontoeröffnung für die Nutzer keine Legitimationsprüfung wie das Postident-Verfahren vor. Banken führen stattdessen bei deutschen Kunden eine Schufa-Abfrage durch und verlangen darüber hinaus evtl. das Zusenden einer Ausweiskopie per E-Mail.[338] Das Einsenden einer Ausweiskopie ohne Prüfung und Vor-Ort-Präsenz der Person stellt keine starke Identitätsprüfung dar und ist zudem in vielen Fällen unzulässig.[339] Mit einer Ausweiskopie werden in jedem Fall mehr persönliche Daten erhoben (z. B. auch Foto, Geburtsdatum, Seriennummer und Card Access Number des Ausweises) als der Online-Ausweisfunktion auf Basis eines Berechtigungszertifikats mit eingeschränkten Zugriffsrechten. Abgesehen davon stellt eine Ausweiskopie auch aus rechtlicher Sicht häufig keinen ausreichenden Nachweis dar.

Fazit: Grundsätzlich ist fraglich, ob ein Dienst für das Vererben eines Kontos ein stärkeres Identifizierungsverfahren benötigt als bei der Erstregistrierung des eigentlichen Kontoinhabers zur Anwendung kommt. Der Identitätsnachweis vor Ort beim Dienstanbieter ist ein starker Identitätsnachweis, der aber

[336] Auch Kreditkarte können als Ausweisdokument dienen, gelten aber als unsicher. Denn Kreditinstitute führen bei der Ausgabe von Kreditkarten nicht unbedingt eine starke Identitätsprüfung der Kunden durch. Zudem sind die Sicherheitsmerkmale amtlicher Ausweise meist fälschungssicherer als die von Kreditkarten.

[337] Die folgenden Postident-Identifizierungsverfahren entsprechen den GwG-Vorgaben: Postfiliale, Videochat und Online-Ausweisfunktion, siehe https://www.deutschepost.de/de/p/postident/sicherheit.html.

[338] Beispielsweise verlangt die Online-Direktbank Advanzia Bank S.A. mit Sitz in Luxemburg unter bestimmten Bedingungen eine Ausweiskopie, siehe https://www.advanzia.com/faq/FAQ.pdf.

[339] Vgl. *Nils Christian Haag*, intersoft consulting services AG, https://www.datenschutzbeauftragter-info.de/ldi-nrw-personalausweis-kopieren-oftmals-nach-dsgvo-verboten.

für beide Seiten aufwendig ist. In vielen Fällen könnte ein einfacherer Identitätsnachweis ausreichen, insbesondere bei kostenlosen Diensten ohne Bezug zu hohen digitalen Werten.

6.8.1.2 Rechtliche Bewertung

Die Vorlage eines Original-Ausweises bei einem Anbieter kann sich für die Verbraucher als schwer durchführbar darstellen. Dies gilt insbesondere dann, wenn der Dienstanbieter seinen Sitz im Ausland hat. Insofern stellen sich dieselben praktischen und tatsächlichen Probleme wie im Rahmen der Vorlage des originalen Berechtigungsnachweises, unabhängig davon, ob sich Erben, Bevollmächtigte oder Betreuer ausweisen müssen.[340] Wenn aufgrund der in Kapitel 6.6.2 auf Seite 232 gefundenen Abwägung auch der Nachweis der Berechtigung lediglich in Kopie oder als Scan vorgelegt werden muss, kann auch die persönliche Vorlage des Ausweises bei einem Anbieter nicht verlangt werden. In einem solchen Fall, und wenn der Dienstanbieter nicht gesetzlich zur Identitätsprüfung verpflichtet ist, könnte auch der Identitätsnachweis durch Vorlage einer Kopie des Ausweises erfolgen, soweit dies aus datenschutzrechtlicher Sicht zulässig ist. Jedenfalls muss die Kopie aber dauerhaft als solche erkennbar sein, § 20 II PAuswG, § 18 III PaßG. Nach dem Grundsatz der Datenminimierung (Art. 5 I c DSGVO) dürfen die Dienstanbieter zudem nur die Daten erheben, die für den Zweck der Identifikation angemessen und erheblich sind. In der Regel wird für den Dienstanbieter ausreichend sein, wenn er Vorname, Name und Geburtsdatum des Berechtigten erkennen kann. Insofern ist der Verbraucher unbedingt auf die Möglichkeit der Schwärzung der nicht benötigten Daten hinzuweisen.

Erneut ist jedoch darauf hinzuweisen, dass der Dienstanbieter dann ein besonderes Interesse an einem Identitätsnachweis im Rahmen der Rechtsnachfolge bzw. Stellvertretung vorbringen muss, wenn er im Rahmen der Eröffnung eines Nutzerkontos keinen Identitätsnachweis verlangt. Hier können allerdings erneut aus Sicht der Anbieter haftungs- oder datenschutzrechtliche Gesichtspunkte eine Rolle spielen.

6.8.2 Identifikation über den Zugriff auf E-Mail-Konten

6.8.2.1 Technische Darstellung und Bewertung

Dienstanbieter könnten vorsehen, dass sich Erben über den Zugriff auf ihre E-Mail-Konten identifizieren. Dies wird dadurch erreicht, dass der Dienstanbieter eine E-Mail mit Link an die E-Mail-Adressen sendet und von den Kontoinhabern – in diesem Fall den Erben – erwartet, den Zugriff durch Klick auf den Link zu bestätigen. Viele Dienste bieten allerdings den Erblassern nicht die Möglichkeit, die Namen und E-Mail-Adressen von Vertrauenspersonen und Erben vorab im Konto zu hinterlegen. Ohne Hinterlegung der E-Mail-Adressen geschieht es häufig, dass die bis dahin namentlich unbekannten Erben dem Dienstanbieter den Sterbefall des Erblassers mitteilen und ihre Berechtigung am digitalen Nachlass nachweisen. Erst auf diesem Weg werden dann ggf. die E-Mail-Adressen der

[340] Siehe hierzu bereits ausführlich oben.

Erben dem Dienstanbieter bekannt gemacht. Allerdings stellt eine nachfolgende alleinige Identifizierung über den Zugriff auf E-Mail-Konten keine starke Identitätsprüfung der Erben dar. Denn die meisten E-Mail-Provider verlangen bei der Einrichtung eines E-Mail-Kontos keine solche Identitätsprüfung. Beispielsweise ist das Vorzeigen eines Personalausweises in der Regel dafür nicht nötig. E-Mail-Provider erteilen auch nicht anderen Dienstanbietern Auskunft über Inhaber der von ihnen verwalteten E-Mail-Konten, sodass eine unabhängige Bestätigung der Zuordnung von Erben zu E-Mail-Adressen schwierig zu bekommen ist.

Jede E-Mail-Adresse ist zwar weltweit eindeutig, enthält aber keine eindeutigen Merkmale, um die Identität des Kontoinhabers gegenüber einem Dritten nachzuweisen. Der vordere lokale Teil der E-Mail-Adresse (d. h. der Adressteil bis zum @) kann beliebige Namen oder Pseudonyme aufweisen. Da viele Anbieter die namentliche Identität der Kontoinhaber nicht validieren, ist es möglich, sich ein E-Mail-Konto unter falschem Namen zuzulegen. Auch ist bei manchen Anbietern die Einrichtung von Alias-Adressen und zeitlich begrenzt gültigen Wegwerf-E-Mail-Adressen möglich.[341] Dienste, für die die Nutzer ihre E-Mail-Adresse verwenden, die aber keine weiteren Identitätsnachweise vorschreiben, versenden bei der Erstregistrierung einen zufälligen Bestätigungscode an die vom Antragsteller angegebene E-Mail-Adresse, um diese Adresse sowie die Zuordnung der Adresse zum Nutzer zu validieren. Im Falle des digitalen Nachlasses reicht dies für den Identitätsnachweis der Erben aber nicht unbedingt aus, weil die Zuordnung der E-Mail-Adresse zu einer bestimmten persönlichen Identität nicht nachgewiesen ist.

Fazit: Die alleinige Prüfung, ob eine Person Zugriff auf ein bestimmtes E-Mail-Konto hat, ist keine ausreichende Identitätsprüfung, da die Online-Dienstanbieter des zu vererbenden Nachlasses darüber Personenangaben nicht zuverlässig ermitteln können. Selbst wenn ein Dienstanbieter den Nachweis der Erbberechtigung mit den Namen eines Erbberechtigten kennt, kann er sich nicht sicher sein, dass eine auf anderem Wege mitgeteilte E-Mail-Adresse wirklich zu diesem Erbberechtigten gehört. Umso bedenklicher ist, dass bei einem nachfolgenden evtl. unberechtigten Zugriff auf das Nutzerkonto des Erblassers die im Konto hinterlegten Daten geändert oder auch gelöscht werden können. Mehr Sicherheit wäre gegeben, wenn die E-Mail-Adressen der Erbberechtigten auch im Berechtigungsnachweis genannt sind, sodass der Dienstanbieter die Adressen eindeutig bestimmten Personen zuordnen kann.

6.8.2.2 Rechtliche Bewertung

Wollen sich dem Dienstanbieter unbekannte Erben identifizieren, so ist allein die Zugriffsmöglichkeit einer Person auf ein E-Mail-Konto wohl nicht ausreichend. Jedenfalls das eigene E-Mail-Konto der Erben kommt als Identitätsnachweis nicht in Betracht, da ein solches einerseits ebenfalls ohne Identitätsprüfung und zudem unter einem Pseudonym oder Kürzel eröffnet werden kann. Denkbar wäre nur, dass es dem Dienstanbieter als Identitätsnachweis ausreicht, dass der (vermeintliche) Erbe auf das E-Mail-Konto des Erblassers zugreifen kann. Allerdings kann dies im Rahmen der erbrechtlichen

[341] Beispielsweise können Nutzer bei Trash-Mail Wegwerf-E-Mail-Postfächer ohne Registrierung und Anmeldung nutzen sowie Fake-E-Mails und anonyme E-Mails versenden, siehe https://www.trash-mail.com.

Übertragung oder des Zugriffs eines Bevollmächtigen nicht als generelle Möglichkeit des Identitätsnachweises empfohlen werden, da zu viele unsichere Faktoren existieren. Zunächst ist es erforderlich, dass der Begünstigte überhaupt auf das E-Mail-Konto des Verbrauchers zugreifen kann, das auch bei dem entsprechenden Dienstanbieter hinterlegt ist. Zudem kann sich auch ein Nichtberechtigter Zugriff auf ein E-Mail-Konto verschaffen, ohne dass der Dienstanbieter dies weiter überprüfen könnte. Bewiesen ist nur die tatsächliche Zugriffsmöglichkeit, nicht jedoch die tatsächliche Identität des Begünstigten. Sinnvoll ist eine Identifikation über die E-Mail-Adresse des Begünstigten nur, wenn diese bereits bei dem Dienstanbieter hinterlegt ist.

6.8.3 Identifikation über digitale Zertifikate

6.8.3.1 Technische Darstellung und Bewertung

Dienstanbieter könnten den Erben anbieten, sich mittels signierter E-Mails oder anderer elektronisch signierter Dokumente zu identifizieren. Bei der elektronischen Signatur mit asymmetrischen kryptografischen Schlüsseln sollte sichergestellt sein, dass ein öffentlicher Schlüssel wirklich zu einer bestimmten Person gehört. Für diesen Zweck gibt es Zertifizierungsstellen, die idealerweise von den beteiligten Kommunikationspartnern als vertrauenswürdig angesehen werden. Eine Zertifizierungsstelle zertifiziert, dass zu einem öffentlichen Schlüssel bestimmte Identitätsdaten des Schlüsselinhabers wie der Name oder die E-Mail-Adresse gehören. Im Kontext elektronischer Signaturen wird das Signaturzertifikat zusammen mit dem signierten Dokument versendet und ist in der Regel auch über öffentliche Verzeichnisdienste zugänglich. Hierbei gilt, dass ein mit der Signatur verbundener Identitätsnachweis maximal so gut sein kann wie die ursprüngliche Erfassung und Prüfung der Identitätsdaten, die in das Zertifikat aufgenommen wurden.

Zertifikate lassen sich grob in 3 Klassen zunehmender Qualität unterteilen. Zertifikate der Klasse 1 beschränken sich über den öffentlichen Signaturprüfschlüssel hinaus auf die geprüfte E-Mail-Adresse des Antragstellers. Für Zertifikate der Klasse 2 muss der Antragsteller zusätzlich eine Ausweiskopie an die Zertifizierungsstelle senden, um Vornamen und Namen in das Zertifikat aufnehmen zu lassen. Dabei werden die Ausweisdaten aber nicht weiter geprüft, d. h. der Antragsteller muss sich nicht persönlich legitimieren. Schließlich setzen Zertifikate der Klasse 3 eine starke Identitätsprüfung der Antragssteller voraus, d. h. in der Regel eine Identitätsprüfung vor Ort, ein Postident-Verfahren oder die Nutzung der Online-Ausweisfunktion.

Die Beantragung einer Signaturkarte für die qualifizierte elektronische Signatur (QES) geht immer mit einer persönlichen Identifizierung des Antragstellers einher. Solche Signaturkarten werden ausschließlich von Anbietern ausgestellt, die gemäß Art. 21 eIDAS-Verordnung akkreditiert sind. Der Karteninhaber kann mit der Signaturkarte elektronische Signaturen erstellen, die gemäß § 126a BGB einer Handunterschrift gleichgestellt sind. Der Empfänger einer QES kann mit der Verifikation der Signatur und des Signaturzertifikats eindeutig die Identität des Signaturerstellers feststellen, zumindest dessen Vornamen und Nachname. Allerdings sollte eine qualifizierte elektronische Signatur nicht

zur reinen Identifizierung eingesetzt werden, „da technisch die Nutzung einer qualifizierten elektronischen Signatur für die Abgabe einer Willenserklärung nicht von einer Nutzung für eine Identifizierung unterschieden werden kann. Damit besteht die Gefahr, dass unabsichtlich eine nicht intendierte Rechtsfolge ausgelöst wird.“[342]

Bei E-Mails, die mit dem Verfahren S/MIME oder OpenPGP signiert wurden, handelt es sich meist um sogenannte fortgeschrittene elektronische Signaturen ohne qualifiziertes Zertifikat. Die jeweilige Zertifizierungsrichtlinie des Anbieters gibt Aufschluss darüber, welche Daten im Zertifikat enthalten sind und wie diese im Rahmen der Zertifikatsausstellung geprüft wurden. Auf dieser Basis könnte der Empfänger eines signierten Dokuments entscheiden, ob er die Signatur als Identitätsnachweis anerkennt. In der Praxis ist es aber für viele Empfänger schlicht nicht nachvollziehbar, ob und wie die Inhalte eines vorliegenden Zertifikats durch die Zertifizierungsstelle geprüft wurden. Es gibt zwar kommerzielle Anbieter von kostenpflichtigen Zertifikaten, die ähnlich wie die Anbieter von Signaturkarten einen starken Identitätsnachweis des Antragstellers (Nutzers) unterstützen. In den meisten anderen Fällen hat aber ein solcher Identitätsnachweis nicht stattgefunden. Zudem werden die Schlüssel in der Regel in der E-Mail-Client-Software oder im Betriebssystem privater Rechner verwaltet, die nicht die gleiche Sicherheit bieten wie hardwarebasierte Signaturkarten.

S/MIME gilt als der Business-Standard für die E-Mail-Verschlüsselung und -Signatur. Zertifikate für S/MIME-Verschlüsselung und -Signatur werden insbesondere von großen Unternehmen verwendet, die eine eigene Public-Key-Infrastruktur (PKI) betreiben oder von einem Zertifizierungsdienstanbieter betreiben lassen („Managed PKI“). Die kryptografischen Schlüssel sind dadurch in der Regel gut geschützt, beispielsweise dadurch, dass sie auf chipbasierten Mitarbeiterkarten gespeichert und nur nach PIN-Eingabe angewendet werden können. Eine herkömmliche PKI auf Basis von X.509-Zertifikaten beruht auf einem hierarchischen Vertrauensmodell, in dem sich verschiedene Zertifizierungsstellen gegenseitig ihre Signaturschlüssel in Form von digitalen Zertifikaten beglaubigen. Auf diese Weise bildet sich eine baumartige Vertrauensstruktur mit einer Wurzel- oder Root-Zertifizierungsstelle als oberster Instanz und verzweigten Zertifikatsketten (Validierungspfaden) bis zu den Zertifikaten der Endteilnehmer. Auf dieser Grundlage funktionieren Identitätsnachweise auf Basis von fortgeschrittenen Signaturen zwischen Mitarbeitern von kooperierenden Unternehmen in der Regel gut.

Im Gegensatz zu hierarchisch ausgestellten S/MIME-Zertifikaten signieren sich die Nutzer von OpenPGP gegenseitig ihre Schlüssel und laden diese Zertifikate selbstständig auf öffentliche Schlüsselserver. OpenPGP beruht also auf einem dezentralen Vertrauensmodell, bei dem die Inhaber der öffentlichen Schlüssel selbst entscheiden, welchen Schlüsseln sie vertrauen und welchen nicht. Durch die getroffenen Einzelentscheidungen bildet sich ein Vertrauensnetz („Web of Trust“) zwischen den Beteiligten, und dies kann zwischen bekannten Personen untereinander gut funktionieren. Viele Nutzer verstehen allerdings die zugrunde liegenden Konzepte nicht. Oft sind auf OpenPGP-Schlüsselservern unter demselben Namen mehrere Schlüssel veröffentlicht. Zudem wird die Nutzeridentität beim Veröffentlichen eines Schlüssels in der Regel nicht überprüft. Daher ist die Vertrauenswürdigkeit von OpenPGP-Zertifikaten schwierig einzuschätzen, wenn sich Sender und Empfänger nicht bereits per

[342] BSI, Technische Richtlinie TR-03107-1, S. 11.

E-Mail-Adresse kennen. Hinzu kommt, dass die technischen Formate S/MIME und OpenPGP hinsichtlich der Signaturen, Schlüssel und Zertifikate nicht miteinander kompatibel sind, sodass sich Kommunikationspartner zunächst darüber verständigen müssten, welches der beiden Verfahren sie verwenden möchten. Sender und Empfänger müssen also dasselbe Verfahren nutzen, wenn sie signierte Nachrichten austauschen und beispielsweise als Identitätsnachweis nutzen möchten.

Fazit: Für einen Dienstanbieter, der unbekannte Personen als Erben identifizieren möchte, ist es aus den oben genannten Gründen schwierig, Signaturen beliebiger Herkunft als Identitätsnachweis anzuerkennen, zumal die qualifizierte elektronische Signatur für Willensbekundungen vorgesehen ist und nicht für den bloßen Identitätsnachweis eingesetzt werden sollte. Hinzu kommt, dass selbst für QES die technische Interoperabilität nicht sichergestellt ist, sodass eine anwendungsübergreifende Verwendung von Zertifikaten unter Umständen nicht funktioniert. Beispielsweise ist nicht sichergestellt, dass Signaturen, die mit einem bestimmten Programm erstellt werden, von beliebigen anderen Programmen geprüft werden können. Oft müssen beide Seiten sogar das gleiche Anwendungsprogramm nutzen, damit es funktioniert, was insbesondere im internationalen Kontext eine sehr hohe Hürde darstellt. Allgemein ist die Verbreitung von elektronischen Signaturen als Willensbekundung und Identitätsnachweis von Personen in der Bevölkerung sehr gering. Auch aus diesem Grund werden Dienstanbieter eine Identitätsprüfung von Nutzern auf Basis von elektronischen Signaturen von sich aus kaum unterstützen.

6.8.3.2 Rechtliche Bewertung

Die qualifizierte elektronische Signatur allein ist kein Mittel zu dem Zweck der Identitätsprüfung einer Person. Eingeführt wurde diese Möglichkeit zur Erleichterung der Abgabe von Willenserklärungen im Rechtsverkehr.[343] Sie ist im deutschen Recht festgehalten in § 126a BGB, nach dem die gesetzlich vorgeschriebene schriftliche Form zur Abgabe einer Willenserklärung durch die elektronische Form ersetzt werden kann, indem eine Erklärung mit dem Namen und der qualifizierten elektronischen Signatur des Erklärenden versehen wird. Da auch technisch nicht unterschieden werden kann, ob die qualifizierte elektronische Signatur lediglich zu Identifikationszwecken oder zur Abgabe einer Willenserklärung erfolgt ist, entsteht die Gefahr für den Verbraucher, dass er im Rechtsverkehr eine Willenserklärung abgibt, obwohl er dies nicht wollte. Dieses Risiko sollte den Verbrauchern nicht unnötig aufgebürdet werden.

Andere elektronische Signaturen, die per E-Mail versendet werden, können meist keinen stärkeren Nachweis der Identität leisten als eine unsignierte E-Mail, da im Rahmen des Signaturverfahrens ebenfalls keine Identitätsprüfung erfolgt. Soweit nicht der jeweilige Dienstanbieter selbst ein Signatur- oder Zertifizierungsverfahren anbietet, das verbraucherfreundlich und leicht nutzbar ist, sind diese technischen Möglichkeiten rechtlich und tatsächlich kaum umsetzbar. Die bestehenden Modelle sind jedenfalls wenig verbraucherfreundlich und technisch sehr aufwendig und können daher nicht als Identifikationsverfahren empfohlen werden.

[343] *Primaczenko/Frohn*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 126a Rn. 1.

6.8.4 Identifikation über Vertrauensdienste

6.8.4.1 Technische Darstellung und Bewertung

Es gibt in Deutschland einige Berufsgruppen, die im Berufsalltag zunehmend qualifizierte elektronische Signaturen nutzen, beispielsweise Notare, Wirtschaftsprüfer, Steuerberater, Ärzte, Standesbeamte und Rechtsanwälte. Einsatzgebiete von QES sind z. B. die Anmeldungen zum Handelsregister durch Notare, die Umsatzsteuervoranmeldungen am Elster-Steuerportal durch Steuerberater, die Einreichung von Dokumenten bei öffentlichen Vergabeverfahren, die Abrechnungen der ärztlichen Leistungen durch Ärzte gegenüber den Abrechnungstellen, die Signatur der Einträge im Personenstandsregister durch Standesbeamte und die Übermittlung von vertraulichen Dokumenten durch Rechtsanwälte an Gerichte und Mandanten. Viele Vertreter dieser Berufsgruppen sind zudem mit der Legitimationsprüfung ihrer Klienten vertraut.

Die in den genannten Berufsgruppen vorhandene Kompetenz könnte für den digitalen Identitätsnachweis von Erben gegenüber Online-Diensten genutzt werden, zumal diesen Berufsgruppen die mit Sterbefällen und Nachlässen verbundenen Themen oftmals schon vertraut sind. Und so könnte der Identitätsnachweis gegenüber einem Online-Dienst gestaltet sein:

(1) Der Notar fertigt eine digitale Kopie des Erbscheins an (ggf. mit Übersetzung) und beglaubigt diese Kopie mit einer qualifizierten elektronischen Signatur.

(2) Der Notar führt eine Legitimationsprüfung der anwesenden Erben durch, dokumentiert und signiert diese Dokumentation.

(3) Der Notar sendet die signierten Dokumente verschlüsselt an den Dienstanbieter und bittet in seinem Schreiben um die Übergabe des digitalen Nachlasses (z. B. Konto des Erblassers) an die Erben.

(4) Der Dienstanbieter prüft die signierten Dokumente und sendet dem Notar eine verschlüsselte signierte Antwort mit neuen temporären Zugriffsdaten zum Konto für die Erben.

(5) Der Notar entschlüsselt die Zugriffsdaten und übergibt sie an die Erben.

(6) Die Erben führen privat mit den Zugriffsdaten den Login durch und ändern und setzen anschließend neue Zugriffsdaten, die nur sie persönlich kennen.

Sender und Empfänger müssten dafür über geeignete Signaturanwendungskomponenten verfügen. Möglicherweise wird ein solcher Signaturprozess zukünftig einfacher und in der EU grenzüberschreitend verfügbarer. Die eIDAS-Verordnung,[344] die zum überwiegenden Teil seit Juli 2016 gilt, wurde mit dem Ziel erlassen, die europaweite Nutzung von elektronischen Identifizierungsverfahren und sogenannten Vertrauensdiensten (für Signaturen, Siegel, Zeitstempel, Zustelldienste, Webseitenzertifikate) zu vereinfachen.

[344] eIDAS (electronic IDentification, Authentication and trust Services) bezeichnet die *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (Signaturrichtlinie)*.

Im Unterschied zur früheren deutschen Signaturrichtlinie erlaubt die eIDAS-Verordnung beispielsweise explizit das Erzeugen und das Verwalten von Signaturschlüsseln durch qualifizierte Vertrauensdienstanbieter, die im Auftrag der signierenden Personen die elektronischen Signaturen erstellen. Damit werden auch serverbasierte Signaturlösungen (Fernsignaturen) möglich. Der Vorteil von Fernsignaturen liegt darin, dass die Nutzer keine zusätzliche technische Ausstattung (Signaturkarte, Lesegerät) benötigen.

Beispielsweise ist die Deutsche Post als qualifizierter Vertrauensdienstanbieter akkreditiert[345] und bietet ein eIDAS- und GwG-konformes sogenanntes e-Signing an. Dazu weist der Nutzer in einem Postident-Videochat seine Identität nach, sendet die zu signierenden Dokumente elektronisch an den Dienst und schaltet schließlich durch die Eingabe einer SMS-TAN den entfernten Signaturprozess frei. Die signierten Dokumente werden zum Download bereitgestellt. Die Signatur gibt Auskunft über die Integrität des Dokuments, den Namen des Signierenden sowie den Zeitpunkt der Signaturerstellung. Die Überprüfung der Signatur ist beispielsweise mit dem Adobe Reader möglich, sodass selbst Online-Dienstanbieter, die nicht auf die Erstellung und Prüfung elektronischer Signaturen vorbereitet sind, die Echtheit der Dokumente überprüfen können. Allerdings wurde nachgewiesen, dass die Validierung von signierten pdf-Dokumenten in vielen pdf-Viewern manipulierbar ist.[346] Ein Grund dafür liegt in der nur mangelhaft beschriebenen Validierungslogik der pdf-Spezifikation und der Toleranz der meisten Validierungsprogramme gegenüber fehlerhaften pdf-Dateien.[347] Zudem ist eine serverseitige eIDAS-Validierungskomponente anfällig für XML-basierte Angriffe.[348]

Fazit: Qualifizierte elektronische Signaturen bieten hohe Sicherheit und Zuordenbarkeit, sind aber in der Praxis anspruchsvoll und nur in bestimmten Berufsgruppen (Notare, Rechtsanwälte etc.) verbreitet. Erben könnten sich an die Vertreter dieser Berufsgruppen wenden, um sich gegenüber den Online-Diensten auszuweisen. Möglicherweise werden sich in den nächsten Jahren eIDAS-Vertrauensdienste etablieren, die vereinfachte und europaweit anerkannte Lösungen anbieten.

6.8.4.2 Rechtliche Bewertung

Grundsätzlich wäre es denkbar, dass Vertrauensdienste die Verbraucher bei der Identifikation gegenüber den Dienstanbietern unterstützen.

Allerdings wären für die soeben vorgeschlagene Lösung des Identitätsnachweises durch Notare rechtlich noch einige Voraussetzungen zu schaffen. Zunächst ist festzuhalten, dass zwar Notare gemäß §§ 39, 39a BeurkG Beglaubigungen elektronisch errichten können. Allerdings ist für die Erteilung von Abschriften und Ausfertigungen eröffneter letztwilliger Verfügungen und Erbscheine das zuständige Nachlassgericht zuständig, nicht ein Notar. Eine entsprechende Vorschrift, die die Zuständigkeit

[345] Weitere akkreditierte Anbieter sind D-TRUST, DGN Deutsches Gesundheitsnetz, Deutsche Telekom, Bundesnotarkammer, Bundesagentur für Arbeit und medisign, siehe Liste der Vertrauensdienstanbieter mit Sitz in Deutschland: https://webgate.ec.europa.eu/tl-browser/#/tl/DE.

[346] *Mladenov u. a.*, 1 Trillion Dollar refund – How to spoof PDF signatures, in: 2019 ACM SIGSAC, S. 1–14.

[347] Siehe Webseite der Ruhr-Universität Bochum: https://www.pdf-insecurity.org.

[348] *Engelbertz u. a.*, Security analysis of XAdES validation in the CEF Digital Signature Services (DSS), in: Open Identity Summit 2019, S. 95–106.

von Notaren zur Beglaubigung von Abschriften eröffneter letztwilliger Verfügungen oder Erbscheine regelt, müsste insoweit erst geschaffen werden. Möglich wäre es im Hinblick auf die vorgeschlagene Lösung aber, dass der Notar eine einfache (digitale) Kopie der erbrechtlich relevanten Urkunde erstellt. Allerdings ist dann der Beweiswert der Urkunde geschmälert. Auch ist eine reine Identitätsprüfung der Anwesenden durch Notare im BeurkG nicht vorgesehen. Diese erfolgt nur in Zusammenhang mit einer Beurkundung von Willenserklärungen, § 10 I BeurkG. Auch im Rahmen der Beglaubigung einer Unterschrift erfolgt zwar eine Prüfung der Identität der Anwesenden, §§ 40 IV i. V. m. 10 I BeurkG. Allerdings werden auch Unterschriften in der Regel nur beglaubigt, wenn ein dazugehöriger Text vorliegt. Eine Ausnahme für Blanko-Unterschriften bildet nur § 40 V BeurkG. Diese gilt aber nur, wenn dargelegt wird, dass die Beglaubigung vor der Festlegung eines Urkundeninhalts benötigt wird. Somit steht die Identitätsprüfung in einem anderen Zusammenhang. Eine Vorschrift, die eine reine Identitätsprüfung vorsieht, müsste somit entweder erst geschaffen werden oder die Identitätsprüfung im Rahmen der Beglaubigung stattfinden. Zu beachten ist aber, dass selbst wenn eine Zuständigkeit von Notaren für die Erteilung beglaubigter Abschriften von letztwilligen Verfügungen oder Erbscheinen besteht, im Rahmen der Beglaubigung (§ 42 BeurkG) nach der geltenden Regelung nicht zwingend eine Identitätsprüfung erfolgt.

Grundsätzlich ist der Notar auch gesetzlich nicht verpflichtet, Erben bei der Abwicklung des Nachlasses zu unterstützen. Zwar bewahrt er notarielle Urkunden auf und leitet diese nach der Sterbefallmitteilung an das zuständige Nachlassgericht weiter, eine grundsätzliche Weiterleitung von Urkunden an Dritte ist aber nicht vorgesehen. Gegebenenfalls könnte diese Aufgabe nur unter die vorsorgende Rechtspflege gefasst werden, zu deren Übernahme der Notar aber in der Regel nicht verpflichtet ist. Nach derzeitiger Rechtslage ist somit eine solche Aufgabenerfüllung durch Notare als Vertrauensperson nicht vorgesehen. Besteht aber ein rechtliches und tatsächliches Interesse an der Übernahme derartiger Aufgaben durch Notare, könnten die gesetzlichen Voraussetzungen wohl geschaffen werden. Zusätzlich wäre aber erforderlich, dass die Dienstanbieter sich überhaupt zur Nutzung entsprechender Verfahren bereit erklären und diese zur Verfügung stellen.

Solange auch eine Identitätsprüfung durch andere Vertrauensdienste – wie im Rahmen des Postident-Verfahrens der deutschen Post (s. o.) – durchgeführt wird, ist jedoch die Schaffung einer solchen Kompetenz für Notare wohl nicht erforderlich.

6.8.5 Identifikation über Telefonnummern

6.8.5.1 Technische Darstellung und Bewertung

Dienstanbieter könnten den Erben anbieten, sich telefonisch unter Nutzung ihrer eigenen Telefonnummer zu identifizieren. Viele Dienste nutzen das beispielsweise in Zusammenhang mit dem Versenden einer E-Mail, um den Zugriff auf einen in der E-Mail mitgeteilten Link zusätzlich durch die Eingabe eines Bestätigungscodes abzusichern. Der Bestätigungscode wird dazu per SMS an das

Telefon des Nutzer gesendet. Die Kontaktdaten E-Mail-Adresse und Telefonnummer müssen allerdings schon zuvor vom Nutzer hinterlegt worden sein. Die Telefonnummer dient nicht dazu, einen bis dahin unbekannten Nutzer zu identifizieren.

Der Zugriff auf ein Festnetz- oder Mobiltelefon lässt sich leichter einer bestimmten Person zuordnen als der Zugriff auf ein privates E-Mail-Konto. Zumindest eine Mobiltelefonnummer lässt sich relativ eindeutig einer Person zuordnen. Denn ein Mobiltelefon wird in der Regel persönlich vom Nutzer mitgeführt und mehrmals täglich kontrolliert. Nutzer müssen sich zum Abschluss eines Mobilfunkvertrags gemäß § 111 TKG ausweisen. Dies gilt seit Juli 2017 auch zur Freischaltung einer gekauften Prepaid-SIM-Karte. Die Identitätsprüfung erfolgt in diesem Fall per Postident. Wird die Prepaid-Karte in einem lokalen Mobilfunkshop gekauft, kann sich der Nutzer wie beim Abschluss eines normalen Mobilfunkvertrags direkt vor Ort mithilfe eines gültigen Ausweises identifizieren. Die Mobilfunkanbieter speichern in der Regel als Bestandsdaten ihrer Kunden Vornamen und Nachnamen, Anschrift, Geburtsdatum, Telefon und Faxnummer, E-Mail-Adresse und die Bankverbindungsdaten.[349] Das gleiche gilt für Festnetzanschlüsse. Hier werden allerdings an jeden Haushalt in der Regel mehrere Nummern vergeben. In einem Haushalt können mehrere Personen leben, die über die Jahre wechseln. Die Festnetznummern sind nicht immer eindeutig einer bestimmten Person zuordenbar.

Online-Dienstanbieter könnten zum Zweck der Identitätsprüfung von Erben Anfragen an Telekommunikationsanbieter stellen, welchen Personen bestimmte Festnetz- oder Mobilfunknummern zugeordnet sind. Dazu müsste zunächst für jede Telefonnummer die Netzzugehörigkeit, d. h. der aktuelle Anbieter bestimmt werden, da es möglich ist, bei einem Vertragsabschluss die eigene Telefonnummer beizubehalten, d. h. die Nummer zu einem anderen Anbieter zu portieren. Mittels Online-Telefonbuch lassen sich Rufnummern durch die sogenannte Rückwärtssuche (Inverssuche) ermitteln. Jedoch können Nutzer gegen eine Verwendung ihrer eigenen Daten in der Inverssuche Widerspruch einlegen. Die Telekommunikationsanbieter sind zudem anderen Dienstanbietern und Privatnutzern gegenüber nicht gesetzlich verpflichtet, Auskunft zu erteilen. Oftmals tun sie dies aus vertraglichen und datenschutzrechtlichen Gründen nicht. Die Auskunft ist in § 105 TKG geregelt und darf nur erfolgen, wenn der Nutzer der Aufnahme in ein Telefonbuch zugestimmt hat. Darüber hinaus bietet die Bundesnetzagentur ein automatisiertes Auskunftsverfahren, allerdings ausschließlich für gesetzlich berechtigte Stellen (z. B. Strafverfolgungsbehörden).[350]

In der Praxis werden Festnetz- und Mobilfunkverträge oftmals von anderen Personen übernommen, z. B. Nachmietern, Untermietern, Erben oder Bekannten des vertraglichen Nutzers, ohne dass die Telekommunikationsanbieter über den Personenwechsel informiert werden. Auch Namensänderungen bei Eheschließungen werden den Anbietern nicht immer mitgeteilt, oder sie werden fehlerhaft aktualisiert. SIM-Karten können unter der Hand weiterverkauft oder verschenkt werden. Aus den genannten Gründen besteht keine Sicherheit, dass die vom Erblasser beim Online-Dienstanbieter hinterlegten

[349] Verbraucherzentrale Niedersachsen, Mobilfunk und Datenschutz, https://www.verbraucherzentrale-niedersachsen.de/sites/default/files/medien/166/dokumente/Mobilfunk_und_Datenschutz_-_So_sch%C3%BCtzen_Sie_Ihre_Daten_bei_Mobilfunkvertr%C3%A4gen.pdf.

[350] Bundesnetzagentur, Rufnummern – So erhalten Sie Auskunft über Anrufer, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/Serviceheft.pdf?__blob=publicationFile&v=3.

Kontaktdaten auch nach Jahren noch korrekt sind und zu einer angegebenen Vertrauensperson gehören. Dienstanbieter können sich bei einem Anruf von einer bestimmten Telefonnummer nicht darauf verlassen, dass es sich bei der anrufenden Person, die sich möglicherweise als Erbe ausgibt, tatsächlich um die Person handelt, die in einem Erbnachweis genannt wird oder vom Erblasser als Vertrauensperson eingetragen wurde.

Fazit: Die Zuordnung von Telefonnummern zu Personen ist fehleranfällig und bleibt über die Jahre nicht immer korrekt. Die Dienstanbieter können sich nicht darauf verlassen, das evtl. vorhandene Kontaktdaten tatsächlich zu den Erben gehören oder dass sich bei einem Anruf von einer bestimmten Telefonnummer eine Person korrekt identifizieren lässt. Die Telekommunikationsanbieter geben nur Auskunft über diejenigen Personen, die der Aufnahme ihrer Daten in ein Telefonbuch zugestimmt haben.

6.8.5.2 Rechtliche Bewertung

Eine Telefonnummer eignet sich dann nicht zur Identifikation eines Begünstigten, wenn dieser dem Dienstanbieter noch gänzlich unbekannt ist. Insofern kann auf die Ausführungen in Kapitel 6.8.2 auf Seite 264 hinsichtlich der Zugriffsmöglichkeit auf eine E-Mail-Adresse verwiesen werden.

6.8.6 Identifikation über Payment und Single Sign-On

6.8.6.1 Technische Darstellung und Bewertung

Der Online-Dienstanbieter könnte auf seiner Micropayment-Webseite die Begünstigten auffordern, zum Nachweis ihrer Identität 1 Cent auf das vom Dienstanbieter angegebene Konto zu überweisen. Die Begünstigten geben ihre jeweilige Micropayment-PIN ein und autorisieren damit die Überweisung. Damit kann über das Micropayment die Identität von Personen verifiziert werden, falls der Micropayment-Anbieter dem Dienstanbieter entsprechende Nutzerdaten mitteilt. Allerdings bleibt bei vielen Micropayment-Verfahren der Endnutzer gegenüber dem Zahlungsempfänger weitestgehend anonym. PayPal sieht bei der Eröffnung eines Geschäftskontos eine Bestätigung der Bankverbindung vor, indem die registrierende Person einen Zahlencode anfordern muss. Nach 2–3 Tagen erhält die Person den Zahlencode im Überweisungstext einer Micropayment-Überweisung auf ihr Bankkonto und muss den Code in ihrem PayPal-Konto unter „Bankkonto bestätigen“ eingeben.

PayPal bietet den Dienstanbietern, die ein PayPal-Geschäftskonto besitzen, den Zugriff über einen RESTful API Web Service auf bestimmte Identitätsdaten der Endnutzer an wie Name, E-Mail- und postalische Adresse mit Angabe, ob – aber nicht, auf welche Weise – diese Daten von PayPal validiert wurden. Mit Option „Connect with PayPal“ kann der Dienstanbieter seinen Dienst so gestalten, dass

sich Nutzer mit ihren PayPal-Logindaten beim Dienst anmelden können. Damit kann der Dienstanbieter Nutzerdaten von PayPal abrufen, mit denen Formulare vorausgefüllt oder vorhandene Daten validiert werden können.[351]

Auch Google, Facebook, Twitter und Amazon bieten Dienstanbietern ein ähnliches Identifikationsverfahren, das auch als Single Sign-On (SSO) bezeichnet wird. So können Dienstanbieter das Social Plugin „Facebook Login“ in Form eines „Mit Facebook anmelden“-Buttons in ihre Web-Anwendungen integrieren. Die Nutzer können sich dann in eine Web-Anwendung einloggen, indem sie sich wie gewohnt über Facebook anmelden, vorausgesetzt, dass sie über ein Facebook-Profil verfügen. Auf diese Weise werden Facebook und die Anwendung miteinander verknüpft und in der Anwendung ist kein separater Login mehr notwendig. Abhängig von den persönlichen Datenschutzeinstellungen bei Facebook werden die im Facebook-Profil allgemeinen und öffentlich zugänglichen Informationen (z. B. Anrede, Vorname, Nachname, Adressdaten, Land, E-Mail-Adresse, Geburtsdatum, Profilbild, Gefällt-mir-Angaben, Freundesliste) von Facebook an den Dienstanbieter übertragen und können sowohl zum Login als auch zur Erstellung eines neuen Kundenkontos verwendet werden.

Umgekehrt werden Nutzerdaten (z. B. Informationen zum Surfverhalten) von der Anwendung an das Facebook-Profil des Nutzers übertragen, dort im Profil angezeigt und zu Werbezwecken ausgewertet. Dies ist aus Datenschutzsicht bedenklich, da auf diese Weise der SSO-Anbieter Facebook weitere personenbezogene Daten sammelt. Zudem sind SSO-Lösungen grundsätzlich als sicherheitskritisch zu bewerten, weil ein erfolgreicher Angriff auf einen SSO-Anbieter möglicherweise den Nutzer-Login auch zahlreicher anderer Dienste kompromittiert.[352] Anbietern, die einen SSO-Button in ihre Anwendung integriert haben, können sich zudem nicht darauf verlassen, dass der SSO-Anbieter bei der Erstregistrierung der Nutzer die Identitätsdaten wie Name, Adresse etc. in einer starken Identitätsprüfung validiert hat.

Um eine von den amerikanischen Diensten unabhängige SSO-Lösung zu schaffen, haben deutsche Unternehmen gemeinsam den Dienst Verimi[353] gegründet, der zudem starke Identitätsprüfungen unterstützt. Verimi wurde 2017 in Deutschland von international tätigen Unternehmen[354] als europäische Identitäts- und Vertrauensplattform für mobile Dienste, Onlinebanking, E-Government und andere Online-Dienste gegründet. Privatnutzer können sich bei Verimi registrieren, ihre personenbezogenen Angaben über die Online-Ausweisfunktion (siehe Kapitel 6.8.8 auf Seite 277) oder einen Videochat verifizieren oder bereits bestätigte Daten aus einem anderen Konto importieren. Eine pseudonyme Nutzung wird ausgeschlossen. Anschließend können die Nutzer das Verimi-Konto mit ihren Konten

[351] Siehe PayPal Identity API, https://developer.paypal.com/docs/connect-with-paypal.

[352] *Ghasemisharif u. a.*, O single sign-off, where art thou? an empirical analysis of single sign-on account hijacking and session management on the web, in: 27th USENIX Security Symposium, S. 1475–1492.

[353] Verimi: https://verimi.de/de.

[354] Zum Gesellschafterkreis von Verimi gehören: Allianz, Axel Springer, Bundesdruckerei, Core, Daimler, Deutsche Bahn, Deutsche Bank und Postbank, Deutsche Telekom, Giesecke+Devrient, Here Technologies, Lufthansa, Samsung Electronics und Volkswagen Financial Services. Die Verimi-Daten werden auf Servern in Deutschland und Europa gespeichert. Online-Dienstanbieter können sich relativ leicht auf Basis von OAuth 2.0 und OpenID Connect an Verimi anbinden, wodurch beide Seiten wiederholte Identifizierungs- und Authentifizierungsprozesse vermeiden können. Bisher ist allerdings keiner der international großen Online-Dienstleister wie Google, Amazon, Facebook oder Apple ein Partner von Verimi.

bei Verimi-Partnern verknüpfen, um sich diensteübergreifend einzuloggen (Single Sign-On) und online auszuweisen. Jedes Konto kann durch eine Zwei-Faktor-Authentisierung (z. B. mit Gesichterkennung oder Fingerabdruckprüfung) zusätzlich abgesichert werden. Der Anspruch von Verimi ist dabei, dass die Privatnutzer besser die Kontrolle darüber behalten, welcher Dienstanbieter auf welche Identitätsdaten zugreifen darf.

Fazit: Über die Integration von Payment- und SSO-Diensten können Dienstanbieter Zugriff auf bei anderen Diensten vorhandene Nutzerdaten bekommen und auf diese Weise Nutzerdaten validieren. Die zugrunde liegenden Nutzerdaten sind aber meist nicht für einen Identitätsnachweis geeignet, weil die Dienstanbieter die Herkunft und Validierung der Daten beim SSO-Anbieter nicht transparent nachvollziehen können. Außerdem gelten die SSO-Dienste der großen amerikanischen Anbieter hinsichtlich Datenschutz und Sicherheit als fragwürdig.

Der Identitätsnachweis von Erben gegenüber den Dienstanbietern mithilfe des SSO- und Identifizierungsdienstes Verimi ist verlässlicher und möglicherweise auch datenschutzfreundlicherer als die Nutzung der üblichen Social Plugins. Allerdings entsteht mit Verimi ebenfalls eine zentrale Datenbank mit umfänglichen Nutzerdaten, und die Verimi-Partnerunternehmen haben es darüber einfacher, die Einwilligung der Nutzer in die Datenverarbeitung einzuholen.[355] Auch ist die Zahl der beteiligten Unternehmen und der Nutzer bisher eher gering.

6.8.6.2 Rechtliche Bewertung

Das Micropayment-Verfahren eignet sich zur Identitätsprüfung nur, wenn Dienstanbieter und Micropayment-Anbieter kooperieren oder wenn der Dienstanbieter selbst das Micropayment-Verfahren durchführt (wie bspw. PayPal). Im ersteren Fall müsste jedoch der Endnutzer sein Einverständnis mit der Weitergabe seiner Daten erklären. In allen anderen Fällen bleibt die Person, die die Überweisung tätigt, gegenüber dem Dienstanbieter anonym. Einen entsprechenden Auskunftsanspruch gegen den Micropayment-Anbieter kann der Dienstanbieter nicht geltend machen. Denkbar wäre nur, dass der Endnutzer die erforderlichen Kontaktdaten im Verwendungszweck der Überweisung angibt. Allerdings ist auch dann erneut für den Dienstanbieter nicht überprüfbar, ob die angegebenen Daten korrekt sind.

Die Identifikation über Single Sign-On-Anwendungen eignet sich aus rechtlicher Sicht zur Identifikation dann, wenn diese Anwendung über einen vertrauenswürdigen Dienst zur Verfügung gestellt wird. Die Anwendung über einen Social-Media-Account eignet sich deshalb in der Regel nicht, weil auch der Dienstanbieter des Social-Media-Portals bei der Anmeldung keine Identitätsprüfung vornimmt. Der Nutzer könnte somit falsche Angaben tätigen oder Pseudonyme verwenden, die eine Identitätsprüfung erneut unmöglich machen. Auch unter Datenschutzgesichtspunkten kann diese Möglichkeit nicht empfohlen werden.

[355] netzpolitik.org e. V., Eine Identität für alles: Das schwierige Geschäftsmodell von Verimi, https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi.

Diese Bedenken tragen aber weitestgehend nicht im Rahmen einer Nutzung des Dienstes Verimi. Dieser Dienst bietet grundsätzlich eine verlässliche Möglichkeit der Identifikation. Kritisch ist lediglich auch hier zu sehen, dass Daten der Nutzer in der zentralen Datenbank von Verimi gespeichert werden. Allerdings erklärt sich der Nutzer durch die Registrierung bei einem solchen Dienst in der Regel mit der Datenspeicherung einverstanden. Zudem ist im Rahmen der praktischen Anwendung erforderlich, dass der jeweilige Dienstanbieter mit Verimi kooperiert. Dies ist insbesondere bei den großen amerikanischen Anbietern infrage zu stellen, insbesondere da diese häufig selbst eine Single Sign-On-Anwendung zur Verfügung stellen.

6.8.7 Identifikation über Ident-Services

6.8.7.1 Technische Darstellung und Bewertung

Postident[356] der Deutschen Post bietet Dienstanbietern verschiedene Verfahren an, in denen die Post im Auftrag des jeweiligen Dienstanbieters Identitäts- und Legitimationsprüfungen gemäß GwG durchführt. Die Verfahren werden nicht vom Endnutzer, sondern vom jeweiligen Dienstanbieter initiiert. Das bedeutet, dass Nutzer nicht von sich aus zur Post gehen können, um einen Identitätsnachweis durchführen zu lassen und anschließend das Ergebnis einem Dienstanbieter vorzulegen. Die Nutzer können aber am Postid-Portal Identitätsdaten für zukünftige Identitätsprüfungen hinterlegen. Alle Postident-Verfahren sind für die Nutzer kostenlos. Als Legitimationsprüfung gemäß GwG sind die folgenden drei Postident-Verfahren anerkannt: Offline-Verfahren in der Postfiliale, Videochat und Online-Ausweisfunktion.[357]

Für das offline Postident-Verfahren in einer Postfiliale muss der Dienstanbieter einen personalisierten Postident-Coupon an den Nutzer senden. Der Nutzer geht in eine Postfiliale, wo ein Mitarbeiter den Identitätsnachweis durch den Scan des mitgebrachten Coupons startet. Der Nutzer weist sich mit einem Personalausweis oder Reisepass aus. Die vom Mitarbeiter verifizierten Daten werden durch Unterschrift des Nutzers und des Mitarbeiters bestätigt und in einem verschlossenen Umschlag an den Dienstanbieter versendet.

Das zweite Verfahren, Postident-Videochat, wird auf der Webseite des Dienstanbieters gestartet, der Nutzer wird zum Postid-Portal weitergeleitet. Dort gibt der Nutzer die persönlichen Daten ein. Über die Webcam führt ein Call-Center-Agent durch das Videochat-Verfahren, prüft die Ausweisdaten und erstellt Fotos. Der Nutzer muss mit der Eingabe einer SMS-TAN den Prozess bestätigen. Das dritte Verfahren, Postident mit der Online-Ausweisfunktion, startet ebenfalls auf der Webseite des Dienstanbieters. Der Nutzer wird zum Postid-Portal weitergeleitet und wählt dort zwischen der Identifikation über Desktop oder per Android-App. Die eID-Daten werden schließlich dem Dienstanbieter über ein Postident-Auskunftsportal oder eine automatische Datenschnittstelle zur Verfügung gestellt.

[356] Postident, https://www.deutschepost.de/de/p/postident.html.

[357] Weitere Anbieter von Ident-Services sind die Paketdienste DHL (offline-Verfahren) und Hermes (offline-Verfahren) sowie IDnow mit einem GwG-konformen Online-Verfahren per Video-Chat.

Fazit: Die Postident-Verfahren und andere Ident-Services sind relativ datenschutzfreundlich und in Deutschland weit verbreitet. Sie sind allerdings meist für die Dienstanbieter kostenpflichtig und werden hauptsächlich dann genutzt, wenn der Dienstanbieter zu einer Legitimationsprüfung seiner Kunden verpflichtet ist oder ein starkes Eigeninteresse an der Identitätsprüfung der Kunden hat.

6.8.7.2 Rechtliche Bewertung

Hat der Dienstanbieter ein Interesse an einem verlässlichen Identitätsnachweis, ist das Postident-Verfahren grundsätzlich eine denkbare und verbraucherfreundliche Alternative. Zu beachten ist allerdings, dass im Rahmen des Verfahrens nur die Daten des Verbrauchers weitergegeben werden dürfen, die für die Identitätsprüfung erforderlich sind, Art. 5 I lit. c DSGVO.[358] Auf dem Postident-Coupon dürfen somit nicht sämtliche Ausweisdaten, sondern nur die notwendigen Angaben vermerkt werden.

Allerdings ist auch hier erforderlich, dass der jeweilige Dienstanbieter dieses Verfahren zur Verfügung stellt. Denkbar ist dieses Verfahren daher vor allem im Rahmen von Vertragsverhältnissen mit Online-Banken, die zumeist ohnehin bei der erstmaligen Kontoeröffnung das Postident-Verfahren anbieten. Insoweit kann auch die Legitimation der Rechtsnachfolger bzw. Stellvertreter durch dieses Verfahren erfolgen, da es bereits im System des Unternehmens integriert ist. In diesem Fall ist die Durchführung des Postident-Verfahrens den Verbrauchern auch zumutbar, da mit den entsprechenden Bankkonten (im Einzelfall hohe) monetäre Interessen verbunden sind. Die Anbieter anderer Dienste sind jedoch nicht wie Banken regelmäßig zur Identitätsprüfung der Nutzer gesetzlich verpflichtet und bieten daher das Postident-Verfahren nicht an. Möglich wäre nur, dass sich ein Dienstanbieter freiwillig vertraglich verpflichtet, dieses Verfahren zur Verfügung zu stellen.

Unter diesen Voraussetzungen kann das Postident-Verfahren daher einen tauglichen Identitätsnachweis gewährleisten.

6.8.8 Identifikation über Online-Ausweisfunktion

6.8.8.1 Technische Darstellung und Bewertung

Die Online-Ausweisfunktion (eID-Anwendung)[359] des Personalausweises und des elektronischen Aufenthaltstitels ist ein elektronischer Identifizierungsdienst, der in Deutschland gemäß §§ 18-21 PAuswG und §§ 28-25 PAuswV gestaltet ist und von staatlicher Seite angeboten wird. Die eID-Anwendung ermöglicht eine sichere gegenseitige Authentisierung von Ausweisinhabern und Dienstanbietern über das Internet, wobei sich die Ausweisinhaber gegenüber Online-Dienstanbietern, die ein Berechtigungszertifikat besitzen, mit den im Zertifikat genannten eID-Datenfeldern ihre Identität nachweisen können. Berechtigungszertifikate müssen beim Bundesverwaltungsamt beantragt und in digitaler

[358] Siehe dazu auch bereits ausführlich oben in Kapitel 6.8.1.2 auf Seite 264.
[359] BSI, Technische Richtlinie TR-03127.

Form beinahe täglich aktualisiert von einem technischen Dienstanbieter (eID-Service-Anbieter) bezogen werden. Die notwendige Anbindung der Web-Anwendungen an die eID-Infrastruktur ist gerade für kleine und mittelständische Online-Dienstanbieter zu Anfang sehr aufwendig und verursacht laufende Kosten.

Die Online-Ausweisfunktion ist nach der eIDAS-Verordnung[360] für die elektronische Identifizierung auf Vertrauensniveau hoch notifiziert[361] und kann somit im gesamten europäischen Wirtschaftsraum zur sicheren Identifizierung eingesetzt werden.

Die Abbildung 6.1 zeigt den Ablauf der Online-Ausweisfunktion zwischen einer Erbin, einem Dienstanbieter, dem gegenüber sie ihre Identität nachweisen möchte, und einem eID-Server der eID-Infrastruktur. Im Beispiel hat der Dienstanbieter die Berechtigung, den Vornamen, Nachnamen und das Geburtsdatum aus dem Ausweis zu lesen. Die Erbin hat die Möglichkeit, die vom Dienstanbieter durch das Berechtigungszertifikat erbetenen Zugriffsrechte weiter einzuschränken.

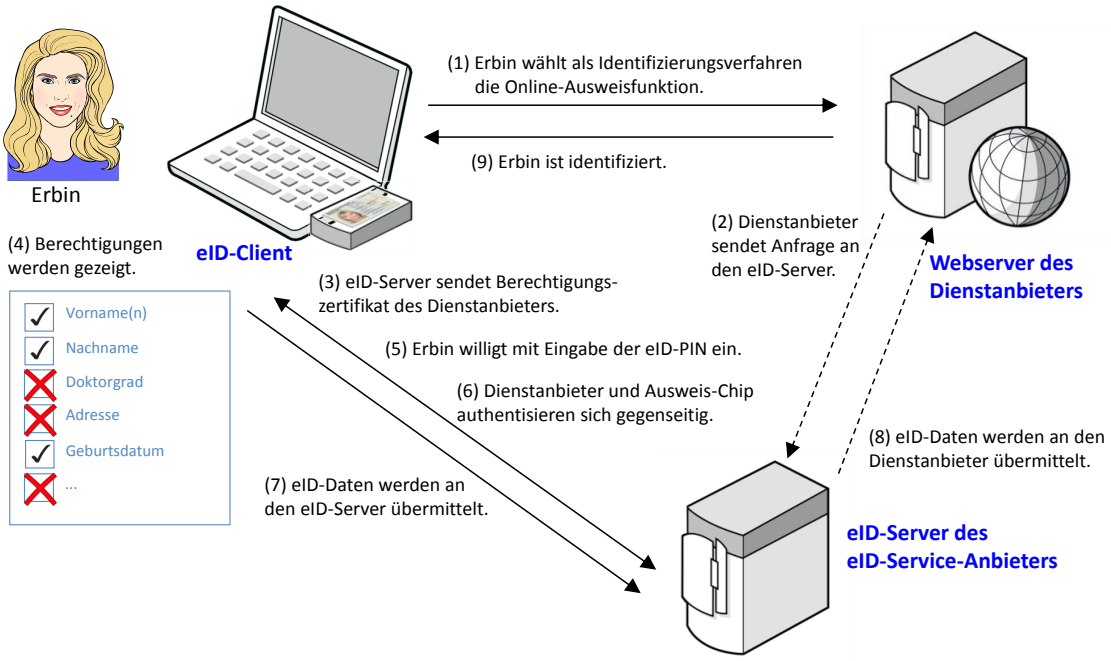

Abbildung 6.1: Ablauf der Online-Ausweisfunktion.

Die folgenden Voraussetzungen müssen erfüllt sein, damit die Erbin die Online-Ausweisfunktion gegenüber einem bestimmten Dienstanbieter nutzen kann:

- Der Dienstanbieter unterstützt die deutsche Lösung der Online-Ausweisfunktion, d. h. er hat bei der Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamts erfolgreich ein Be-

[360] eIDAS (electronic IDentification, Authentication and trust Services) bezeichnet die *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (Signaturrichtlinie)*.

[361] BSI: eIDAS-Notifizierung der Online Ausweisfunktion, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html.

rechtigungszertifikat beantragt und hat seinen Online-Dienst technisch an die eID-Infrastruktur angebunden.

- Die Erbin hat bei Abholung ihres Ausweises die Online-Ausweisfunktion in der Meldebehörde nicht deaktivieren lassen.
- Die Erbin hat eine lokale Client-Software (eID-Client) installiert.
- Die Erbin verfügt über ein Lesegerät für kontaktlose Karten[362] oder hat ein NFC-fähiges Smartphone,[363] das sie als Ausweislesegerät nutzen kann.
- Die Erbin hat den PIN/PUK-Brief der Meldebehörde zur Kenntnis genommen und die fünfstellige Transport-PIN ihres Ausweises z. B. mithilfe einer eID-Client-Software erfolgreich in die persönliche 6-stellige eID-PIN geändert.
- Die Erbin hat während der Online-Ausweisfunktion eine stabile Internetverbindung.
- Die Erbin kennt ihre persönliche eID-PIN trotz der wahrscheinlich seltenen PIN-Eingabe.

Die im Ausweischip gespeicherten eID-Daten umfassen Vornamen, Familiennamen, Doktorgrad, Tag und Ort der Geburt, Anschrift (inkl. Postleitzahl) und den amtlichen Gemeindeschlüssel des Wohnortes. Die Ausweisfunktion bietet neben den selektiven eID-Datenfeldern datensparsame Funktionen wie die Pseudonymfunktion, d. h. das dienste- und kartenspezifische Kennzeichen ohne Preisgabe weiterer personenbezogener Daten zur Wiedererkennung einer Person, die Altersverifikation, d. h. die Überprüfung eines Mindestalters ohne Preisgabe des Geburtsdatums, und die Wohnortverifikation ohne Preisgabe der Adresse. Jedes Berechtigungszertifikat eines Dienstanbieters ist an einen bestimmten Anwendungsfall des Dienstes geknüpft und autorisiert zum Zugriff auf ganz bestimmte eID-Datenfelder. Online-Dienste erhalten in der Regel nur wenige Zugriffsrechte, insbesondere nicht auf die postalische Adresse oder das Geburtsdatum, wenn dies für den Anwendungsfall nicht unbedingt notwendig ist.

Zur eindeutigen Identifizierung einer Person im Abgleich mit den Angaben auf dem Erbschein würde die Pseudonymfunktion oder allein Vorname(n) und Familienname vermutlich nicht ausreichen. Die Vererbung eines Kontos würde damit als neuer Anwendungsfall gelten, für den ein weiteres Berechtigungszertifikat erforderlich ist. Dienstanbieter können aber inzwischen die Online-Ausweisfunktion über die Identifizierungsdienste Verimi und Postident der Deutschen Post nutzen, siehe die vorigen Kapitel 6.8.6 auf Seite 273 und 6.8.7 auf Seite 276. Diese Identifizierungsdienstanbieter mussten für ihre umfassenden eID-Berechtigungen für die Online-Ausweisfunktion besondere Zertifizierungsverfahren durchlaufen.[364]

[362] Geeignete Kartenlesegeräte: https://www.ausweisapp.bund.de/kompatible-geraete/kartenlesegeraete.

[363] Geeignete Smartphones und Tablets: https://www.ausweisapp.bund.de/mobile-geraete.

[364] Vgl. dazu die Angaben auf der Seite https://www.personalausweisportal.de/DE/Wirtschaft/Identifizierungsdiensteanbieter_werden/identifizierungsdiensteanbieter_werden_node.html, insbesondere die unter 4. genannten Anforderungen für Identifizierungsdienstanbieter, die wegen der zusätzlichen Auditierung höher sind als bei normalen Dienstanbietern.

Fazit: Die Online-Ausweisfunktion ist ein datenschutzfreundliches Identifizierungsverfahren und bietet ein hohes Sicherheitsniveau. Gerade auch in Verbindung mit Postident oder Verimi kann die Online-Ausweisfunktion auch aus rechtlicher Sicht empfohlen werden. Bisher bieten allerdings nur wenige Dienste ihren Nutzern die Online-Ausweisfunktion an,[365] die großen international verbreiteten Online-Dienste sind nicht darunter. Denn es handelte sich bisher um einen landesspezifischen digitalen Identitätsnachweis. Die Akzeptanz wird sich zumindest im europäischen Wirtschaftsraum verbessern, insbesondere im behördlichen Umfeld, da die Online-Ausweisfunktion Ende September 2017 gemäß eIDAS-Verordnung für das höchstmögliche Vertrauensniveau „hoch“ notifiziert wurde.[366] Europäische Unternehmen können die Online-Ausweisfunktion auf freiwilliger Basis anerkennen.

Die Integrität der persönlichen Daten der Ausweisinhaber ist sehr hoch, da die Ausweisdaten aus den Meldebehörden stammen und direkt vom Ausweischip an den eID-Service übermittelt werden. Allerdings setzt das Verfahren voraus, dass der Dienstanbieter ein Berechtigungszertifikat besitzt und seinen Dienst an die eID-Infrastruktur angebunden hat. Außerdem wird der Anwendungsfall „Vererben“ für eine eindeutige Identifikation der Nutzer in vielen Fällen eine Zugriffsberechtigung auf mehr eID-Datenfelder erfordern als den Diensten für die existierenden Anwendungsfälle genehmigt wurden. Dies würde die Aufwände bei den Dienstanbietern noch erhöhen. Dienstanbieter können aber inzwischen die Online-Ausweisfunktion über die Identifizierungsdienste Verimi und Postident-Verfahren nutzen. Aus Verbrauchersicht ist die Online-Ausweisfunktion wenig benutzungsfreundlich, solange nicht die speziellen Voraussetzungen (eID-Client, Kartenleser, eID-PIN) erfüllt sind. Mit der Unterstützung von mobilen eID-Clients auf Smartphones ist eine Verbesserung in Sicht.

6.8.8.2 Rechtliche Bewertung

Das Verfahren im Rahmen der Online-Ausweisfunktion kann aus rechtlicher Sicht zum Identitätsnachweis empfohlen werden. Zwar ist das Verfahren relativ aufwendig und die Verbraucher können nicht zur Nutzung verpflichtet werden, obwohl die Online-Ausweisfunktion bei neuen Personalausweisen automatisch eingeschaltet ist. Allerdings müssen die Verbraucher selbst die Funktion durch Setzen einer PIN aktivieren. § 18 I 1 PAuswG regelt, dass der Personalausweisinhaber seinen Ausweis lediglich zum elektronischen Nachweis seiner Identität verwenden „kann“. Hat der Verbraucher die Funktion aber aktiviert, kann der Identitätsnachweis auf diesem Weg erfolgen.

Erforderlich ist jedoch auch hier, dass der Dienstanbieter das Verfahren anbietet. Hierzu ist eine Berechtigung i. S. d. § 21 PAuswG erforderlich, die der Dienstanbieter nur unter bestimmten Voraussetzungen und nur befristet erhält. Daher werden die Dienstanbieter selbst in der Regel das Verfahren nicht durchführen. Möglich ist jedoch die Nutzung des Dienstes Verimi oder des Postident-Verfahrens.

[365] Personalausweisportal: Hier können Sie die Online-Ausweisfunktion nutzen, https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html.

[366] BMI: „Durch die Notifizierung sind alle EU-Mitgliedsstaaten seit 29. September 2018 verpflichtet, ihre eigenen Verwaltungsverfahren für die deutsche Online-Ausweisfunktion zu öffnen, wenn sie eine elektronische Identifizierung auf „substanziellem“ oder „hohem“ Vertrauensniveau benötigen.“ https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

Auch diese Möglichkeiten muss der Dienstanbieter jedoch zur Verfügung stellen. Dies wird nur geschehen, wenn der Dienstanbieter ein berechtigtes Interesse an einem derart verlässlichen Identitätsnachweis hat. Dies kommt erneut bei Online-Banken in Betracht, die gesetzlich zur Identitätsprüfung verpflichtet sind.

6.8.9 Vergleich und Bewertung der genannten Verfahren

6.8.9.1 Aus technischer Sicht

Die Tabelle 6.5 vergleicht einige Eigenschaften der genannten Verfahren zur Identitätsprüfung. Die in der Kopfzeile aufgeführten Eigenschaften bedeuten Folgendes: „Qualität“ steht für die Stärke des Identitätsnachweises, dass die Daten korrekt sind und wirklich zu der angegebenen Person gehören. „Einfach (Nutzer)“ bedeutet, dass die Voraussetzungen für das Verfahren bei den meisten Nutzern bereits gegeben sind. Ein Verfahren gilt als „Kostenlos“, wenn die Nutzer sich keine zusätzlichen Geräte beschaffen, keine Reisen machen und keine kostenpflichtigen Verträge abschließen müssen, „Einfach (Anbieter)“ meint, dass der Dienstanbieter keinen hohen Aufwand hat, um das Verfahren anzubieten. „Verbreitung“ macht eine Aussage über die Häufigkeit des Verfahrens und die internationale Anwendbarkeit.

Verfahren	Qualität	Einfach (Nutzer)	Kostenlos	Einfach (Anbieter)	Verbreitung
Vor-Ort/ Kopien	++	o	o	o	+
E-Mail-Konto	– –	++	++	++	++
Dig. Zertifikat	–	o	o	–	o
Vertrauensdienst	+	–	–	o	–
Telefonnummer	–	++	++	++	++
Single Sign-On	o	–	+	+	o
Ident-Service	++	+	o	+	+
Online-Ausweis	++	–	o	–	–

Tabelle 6.5: Identifizierungsmöglichkeiten für der Erben

Keines der genannten Verfahren bietet sowohl umfassende Qualität und Sicherheit als auch Einfachheit und weite Verbreitung, sodass kein Verfahren für die Identitätsprüfung uneingeschränkt empfohlen werden kann. Eine starke Identitätsprüfung und Sicherheit bieten neben der persönlichen Legitimationsprüfung vor Ort nur die GwG-konformen Ident-Services und die Online-Ausweisfunktion, die allerdings auf ihre Weise aufwendig sind. Postident und andere Ident-Services werden relativ häufig verwendet, allerdings meist im Kontext von Diensten, für die eine Legitimationsprüfung der Kunden vorgeschrieben ist. Meist müssen die Dienstanbieter den Ident-Prozess initiieren und dafür zahlen. Für die Online-Ausweisfunktion benötigt der Dienstanbieter eine technische Anbindung an die deutsche eID-Infrastruktur und ein Berechtigungszertifikat, das zum Auslesen bestimmter Datenfelder des

Ausweises berechtigt und beim Bundesverwaltungsamt beantragt werden muss. Dies erfüllen bisher nur sehr wenige Dienste, von denen die meisten zudem auf Deutschland beschränkt sind.

Die folgende Tabelle 6.6 gibt einen Überblick über die Vor- und Nachteile der einzelnen Verfahren zur Identitätsprüfung der Berechtigten.

Tabelle 6.6: Verfahren zur Identitätsprüfung mit ihren Vor- und Nachteilen

Lösung	Vorteile	Nachteile
Identifikation vor Ort oder Ausweiskopien	✓ Klar verständliche Identitätsprüfung ✓ Starke Prüfung vor Ort ✓ Kopien einfach zu erstellen	✗ Nicht in jedem Fall benötigt ✗ Für beide Seiten sehr aufwendig ✗ Ausweiskopien unsicher
Zugriff auf E-Mail-Konten	✓ Voraussetzungen gegeben und unkompliziert	✗ Beweist nur Zugriffsmöglichkeit, nicht tatsächliche Identität ✗ E-Mail-Anbieter geben keine Auskunft ✗ Nur ausreichend, wenn Adresse zuvor aus zuverlässiger Quelle bekannt
	✓ evtl. Zugriffsmöglichkeit auf Konto des Erblassers ausreichend	✗ Kein Identitätsbeweis ✗ Zugriff kann erschlichen sein
Identifikation über digitale Zertifikate	✓ Zertifikatsdaten technisch sicher verifizierbar	✗ Herkunft der Zertifikate schwierig nachzuvollziehen ✗ QES gilt als Willensbekundung, nicht als Identitätsnachweis
	✓ Digitale Signaturen weit verbreitet	✗ Den meisten Anwendungen liegt keine Identitätsprüfung zugrunde ✗ Verschiedene inkompatible Verfahren, nicht benutzungsfreundlich
Identifikation über Vertrauensdienste	✓ Denkbar über Notare, die QES bereits nutzen	✗ Für Verbraucher aufwendig und kostspielig ✗ Reine Identitätsprüfung durch Notare bisher nicht vorgesehen
	✓ eIDAS-Vertrauensdienste europaweit geplant	✗ Meist noch nicht zertifiziert, wenig verbreitet ✗ Dienstanbieter müssen bereits sein, Verfahren zu integrieren
Identifikation über Telefonnummern	✓ Voraussetzungen gegeben und unkompliziert	✗ Zuordnung von Telefonnummern zu Personen fehleranfällig ✗ Telefonanbieter geben nur eingeschränkt Auskunft ✗ Nur akzeptabel, wenn Nummer zuvor aus zuverlässiger Quelle bekannt

Fortsetzung auf der nächsten Seite

Tabelle 6.6: Verfahren zur Identitätsprüfung mit ihren Vor- und Nachteilen (Fortsetzung)

Lösung	Vorteile	Nachteile
Identifikation über Payment und Single Sign-On	✓ Payment und SSO-Plugins sozialer Netzwerke weit verbreitet	✗ Herkunft und Validierung der Daten nicht transparent ✗ Micropayment meist anonym ✗ Identitätsprüfung durch soziale Netzwerke fragwürdig ✗ Datenschutz sozialer Netzwerke fragwürdig
	✓ SSO-Plattform Verimi ist deutsch-europäisch	✗ Zentrale umfängliche Datenbank ✗ Anbieterbeteiligung bisher gering
Identifikation über Ident-Service	✓ Datenschutzfreundlich und verbraucherfreundlich ✓ Starke Identitätsprüfung	✗ Für Dienstanbieter kostenpflichtig ✗ Realistisch nur dann, wenn Anbieter zur Legitimationsprüfung verpflichtet
Identifikation über Online-Ausweis-funktion	✓ Sehr datenschutzfreundlich ✓ Starke Identitätsprüfung ✓ Auch in Verbindung mit Postident und Verimi	✗ Nur in Deutschland und dort nur wenig verbreitet ✗ Aufwendig für Anbieter und Nutzer ✗ Anbieter müssen Interesse daran haben

6.8.9.2 aus rechtlicher Sicht

Als Identitätsnachweis sind aus rechtlicher Sicht grundsätzlich die Kopie eines Ausweises, die Online-Ausweisfunktion und das Postident-Verfahren denkbar.

Die Online-Ausweisfunktion ist als Verfahren in seiner erstmaligen Errichtung für die Verbraucher noch relativ aufwendig. Diesbezüglich stellt sich die Kopie von Ausweisen als einfacheres Verfahren dar. Jedoch ist hier zu beachten, dass Dienstanbieter nicht berechtigt sind, sämtliche durch die Kopie übermittelten Informationen zu erhalten. Die Verbraucher sind daher auf ihr Recht zur Schwärzung nicht relevanter Informationen hinzuweisen. Vorteil des Online-Ausweisverfahrens ist demgegenüber, dass von vornherein nur die Informationen übermittelt werden, die der Dienstanbieter benötigt.

Dies kann auch das Postindent-Verfahren leisten. Dieses Verfahren ist gegenüber der Online-Ausweisfunktion für die Verbraucher auch weniger aufwendig. Allerdings ist erforderlich, dass der Dienstanbieter das Verfahren unterstützt. Dies tun bisher nur die Dienstanbieter, die gesetzlich zu einer Identitätsprüfung verpflichtet sind.

Identitätsprüfung der Erben
Der herkömmliche Weg, sich gegenüber einem Dienstanbieter zu identifizieren, bestand bisher darin, beim Dienstanbieter persönlich zu erscheinen, ein Ausweisdokument und bei Bedarf weitere amtliche Nachweise vorzulegen. Dies kann bei der möglichen Zahl der genutzten internationalen Online-Dienste kaum von den Erben verlangt werden, zumal das Vererben gerade vieler kostenlos angebotener Dienste kaum finanzielle Aufwände erfordern sollte. In Deutschland existiert das für Dienstanbieter kostenpflichtige Postident-Verfahren, das bisher hauptsächlich bei Dienstanbietern zum Einsatz kommt, die zur Legitimationsprüfung ihrer Kunden verpflichtet sind. Die deutsche Online-Ausweisfunktion wird im internationalen Kontext kaum verwendet, da deren Einrichtung sowohl für Dienstanbieter als auch für Nutzer relativ aufwendig ist. Die Bedeutung dieser Verfahren könnte sich aber vergrößern, dadurch dass einige Vertrauensdienste wie Postident und elektronische Identitätsprüfungen wie die Online-Ausweisfunktion inzwischen europaweit anerkannt werden.

6.9 Zusammenfassung

Ein Verbraucher hat somit verschiedene Vorsorgemöglichkeiten in Hinblick auf seine digitalen Inhalte. Dabei kann er sich entscheiden, ob er bereits eine Vorsorge treffen möchte, die bereits zu seinen Lebzeiten im Fall seiner Handlungsunfähigkeit wirkt. In diesem Fall kann der Verbraucher insbesondere einen Vorsorgebevollmächtigten benennen, der ihn vertritt, wenn er nicht mehr handlungsfähig ist. Möchte der Verbraucher keine Vorsorgevollmacht erteilen, aber zumindest bestimmen, wer bei Eintritt der Handlungsunfähigkeit als Betreuer bestellt wird, kann er eine Betreuungsverfügung erstellen.

Stattdessen oder daneben kann der Verbraucher auch eine Vorsorge für den Fall seines Todes treffen. Je nach seinem Regelungsbedürfnis kann er sich hier der verschiedenen erbrechtlichen Verfügungen bedienen und Erben einsetzen, diese mit Auflagen beschweren, Vermächtnisse erteilen oder Teilungsanordnungen bestimmen. Der Verbraucher kann auch entscheiden, dass nach seinem Tod niemand mehr auf seine digitalen Inhalte zugreifen können soll. Um all diese Verfügungen abzusichern, kann der Verbraucher einen Testamentsvollstrecker oder einen Vorsorgebevollmächtigten bestellen.

Zusätzlich ist es aber zu empfehlen, dass der Verbraucher seinen Rechtsnachfolgern bzw. Bevollmächtigten eine Liste seiner digitalen Inhalte, insbesondere von Nutzerkonten bei Online-Dienstanbietern, und die dazugehörigen Zugangsdaten zur Verfügung stellt. Dies sollte nicht im Testament oder in der Vorsorgevollmacht selbst erfolgen, sondern durch Auflistung in einem gesonderten Dokument. Hier bietet sich insbesondere eine mit einem Masterpasswort verschlüsselte Auflistung auf

einem USB-Stick oder sonstigen lokalen Speichermedium an, wobei das Masterpasswort bei einer Vertrauensperson hinterlegt werden kann (Vorsorgeurkunde). Möglich, aber weniger sicher, ist auch die Aufbewahrung einer Liste der Zugangsdaten durch den Verbraucher selbst.

Neben dem Speichern der Zugangsdaten auf USB-Stick wurden weitere technische Verfahren auf ihre Eignung zur Bereitstellung der Zugangsdaten untersucht. Die verbreitete Passwort-Vergessen-Funktion der Online-Dienste bietet keine gute Vorsorgemöglichkeit, um Zugang zu den Konten des Erblassers zu erhalten, da die Funktion allein auf den Kontoinhaber bezogen ist und zudem als unsicher gilt. Passwort-Manager und digitale Datensafes sind als Vorsorgemaßnahmen besser geeignet, wobei es große Unterschiede zwischen den Produkten gibt. Die meisten dieser Produkte sind Serverlösungen, deren hohe Gebrauchstauglichkeit und Verfügbarkeit in der Regel mit einer Verminderung von Sicherheit und Datenschutz einhergehen. Der Passwort-Manager KeePass bildet dabei eine Ausnahme, da die Software lokal genutzt wird und unabhängig von einem Anbieter sicher funktioniert.

Ein weitere Möglichkeit ist die Nutzung eines digitalen Nachlassdienstes zur Vorsorge durch den Erblasser oder ohne Vorsorge im Todesfall durch die Erben. Gerade im letzten Fall können Nachlassdienste nur dann wirklich hilfreich sein, wenn sie sowohl von amtlichen Stellen als auch von den Online-Dienstanbietern akzeptiert sind, d. h. die notwendigen Nachweise beziehen und Anweisungen bei den Online-Diensten durchsetzen können. Die bisherigen Angebote haben allerdings gezeigt, dass Zuverlässigkeit, Langlebigkeit und Akzeptanz der Nachlassdienste eher die Ausnahme sind. Auch die Sicherheit der hinterlegten Daten, insbesondere die Anhäufung von personenbezogenen Daten bei den Anbietern, ist bedenklich. Nachlassdienste, die Zugangsdaten speichern und anbieten, im Todesfall die Daten an die Erben weiterzugeben, können daher wohl nur dann empfohlen werden, wenn der Dienst dem Erblasser Integrität und dauerhafte Leistungsfähigkeit nachweisen kann, was praktisch kaum durchführbar ist.

Eine denkbare umfassende Lösung, die auch die Online-Dienstanbieter direkt mit einbeziehen würde, besteht in einer zentralen staatlich unterstützten Plattform mit den entsprechenden Schnittstellen zu den amtlichen Stellen und zu den Systemfunktionen der Online-Dienste. Eine solche Plattform würde den Erblassern verbindliche Vorsorgemaßnahmen erleichtern und den Erben die Erbringung von Nachweisen vereinfachen. Allerdings wurde eine solche Plattform bisher nicht realisiert, da viele der damit verbundenen technischen, organisatorischen und rechtlichen Fragen noch ungeklärt sind. Zudem stehen die mit einer solchen Plattform verbundenen Vorteile im Vergleich zum Aufwand ihrer Errichtung und Verwaltung infrage. Auch bestehen erhebliche Datenschutzbedenken gegen eine solche zentrale Lösung.

Damit verglichen ist die oben genannte Vorsorgemaßnahme in Form einer Liste der digitalen Nutzerkonten und zugehörigen Zugangsdaten in einem lokalen digitalen Archiv (z. B. USB-Stick) oder auf Papier eine pragmatische und bei guter Durchführung sichere Lösung, die allerdings hauptsächlich in der Verantwortung der Nutzer liegt. Für Erblasser kann es zu Lebzeiten mühsam sein, die Daten über Jahre aktuell zu halten und eine sichere Übergabe der Geräte und Daten vorzubereiten. Aber auch bei dieser Art von Vorsorge sind die Online-Dienstanbieter nicht an der Vorsorge beteiligt und werden regelmäßig erst im Bedarfsfall über die Existenz von Erben und Bevollmächtigten informiert.

Daneben müssen die Erben und Bevollmächtigten ihre Berechtigung im Rechtsverkehr nachweisen. Erben können ihre Berechtigung durch ein eröffnetes Testament oder einen Erbschein nachweisen, ein Vorsorgebevollmächtigter durch die Vollmachtsurkunde und ein Betreuer durch den Betreuerausweis. Dies kann sich insbesondere gegenüber Dienstanbietern mit Sitz im Ausland schwierig darstellen und weitere Probleme bereiten, wenn der Verbraucher bei bestimmten Nutzerkonten ein Pseudonym verwendet hat. Zwar ist es nach hier vertretener Auffassung zumeist – im Rahmen von Vertragsverhältnissen mit keinem oder geringem monetären Bezug – ausreichend, wenn den Dienstanbietern lediglich eine Kopie oder ein Scan der Berechtigungsurkunde vorgelegt wird. Allerdings ist dies davon abhängig, dass die Dienstanbieter diesen Nachweis akzeptieren.

Untersucht wurde daher auch die Frage, ob die erforderlichen Urkunden in digitaler Form vorgelegt werden können, um den Verbrauchern den Nachweis zu erleichtern. Eine originäre digitale Errichtung von letztwilligen Verfügungen und Vorsorgevollmachten ist zwar aufgrund der technischen und rechtlichen Voraussetzungen nicht möglich. Allerdings wird es nach bereits geltender Rechtslage in Zukunft möglich sein, die Beglaubigung erbrechtlicher Urkunden in digitaler Form vorzunehmen, sobald bei den zuständigen Stellen die hierfür erforderliche Infrastruktur vorhanden ist. Eine Anpassung oder Änderung des Zentralen Testamentsregisters ist in diesem Zusammenhang nicht angezeigt. Auch die Ausfertigung von Vorsorgevollmachten in digitaler Form ist technisch bereits möglich. Den hierfür zuständigen Notaren steht zudem bereits die erforderliche Infrastruktur zur Verfügung. Insofern wären aber Anpassungen des Beurkundungsgesetzes erforderlich, da nach der geltenden Rechtslage die Ausfertigung in digitaler Form noch nicht vorgesehen ist. Eine Erweiterung des Zentralen Vorsorgeregisters ist in diesem Zusammenhang nicht angezeigt. Wird das Elektronische Urkundenarchiv aber zukünftig zu einem Vollmachts- und Titelregister weiterentwickelt, könnte dies auch den Nachweis im Rahmen des digitalen Nachlasses erleichtern.

Zusätzlich wurde beleuchtet, wie die Begünstigten ihre Identität nachweisen können, wenn der Dienstanbieter hierüber einen weiteren Nachweis anfordert. Möglich ist, die Kopie eines Ausweises vorzulegen, allerdings haben die Verbraucher in diesem Fall das Recht, für den Dienstanbieter nicht relevante Stellen zu schwärzen. Des Weiteren wurde der Identitätsnachweis über den Zugriff auf E-Mail-Konten, Nutzung von digitalen Zertifikaten und Vertrauensdiensten, Telefonnummern, Payment- und Single Sign-On-Verfahren, Postident und Online-Ausweisfunktion des Personalausweises untersucht. Keines der genannten Verfahren bietet sowohl umfassende Qualität und Sicherheit als auch Einfachheit und weite Verbreitung. So können Dienstanbieter die Begünstigten beispielsweise nicht allein an Telefonnummern und E-Mail-Adressen sicher erkennen, wenn ihnen die Daten nicht zuvor auf sicherem Wege bestätigt wurden.

Eine starke Identitätsprüfung und Sicherheit bieten neben der persönlichen Legitimationsprüfung vor Ort nur die GwG-konformen Ident-Services (z. B. Postident) und die Online-Ausweisfunktion, die allerdings auf ihre Weise aufwendig sind. Ident-Services werden relativ häufig verwendet, allerdings meist im Kontext von Diensten, für die eine Legitimationsprüfung der Kunden vorgeschrieben ist. Meist müssen die Dienstanbieter den Ident-Prozess initiieren und dafür zahlen. Für die Online-Ausweisfunktion benötigt der Dienstanbieter eine technische Anbindung an die deutsche eID-Infrastruktur und ein Berechtigungszertifikat. Dies erfüllen bisher nur sehr wenige Dienste, von denen die meisten zudem auf Deutschland beschränkt sind.

Das Wichtigste in Kürze

» Der Verbraucher hat verschiedene Möglichkeiten, seinen digitalen Nachlass zu vererben. Hierzu ist grundsätzlich die Errichtung eines Testaments erforderlich. Hierbei kann der Erblasser verschiedene Anordnungen treffen:

- Er kann einen oder mehrere Erben einsetzen, die das Recht haben, frei über den digitalen Nachlass zu verfügen und die Daten und Nutzerkonten so zu benutzen, wie auch er selbst dies könnte.

- Möchte der Erblasser bestimmten Personen einen bestimmten digitalen Inhalt zuwenden, so kann er ein Vermächtnis oder eine Teilungsanordnung in seinem Testament festlegen. Grundsätzlich gilt, dass allein durch eine Einsetzung als Erbe keine einzelnen Vermögensgegenstände auf eine bestimmte Person übertragen werden können. Allerdings kann der Erblasser dies steuern, indem er ein Vermächtnis oder eine Teilungsanordnung in seinem Testament vorsieht.

- Um seine Anordnungen abzusichern, kann der Erblasser seine Erben auch mit Auflagen beschweren. Durch eine Auflage kann der Erblasser die Erben anweisen, sich in einer bestimmten Weise zu verhalten. Deshalb kann durch eine Auflage auch bestimmt werden, dass bestimmte Daten (mit oder ohne vorherige Einsicht der Erben) gelöscht werden sollen.

  - Für eine weitere Absicherung der Anordnungen kann auch eine Testamentsvollstreckung angeordnet oder eine über den Tod hinaus wirkende Vollmacht erteilt werden. Der Testamentsvollstrecker bzw. Vollmachtnehmer verwaltet dann den Nachlass im Sinne des Erblassers, bis die Nachlassgegenstände unter den Erben aufgeteilt sind. Testamentsvollstreckung und Vollmacht haben verschiedene Vor- und Nachteile. Grundsätzlich hat der Testamentsvollstrecker gegenüber den Erben die stärkere Position, allerdings kann es einige Zeit dauern, bis er durch ein Nachlassgericht in sein Amt berufen wurde. Ein Vorsorgebevollmächtigter kann demgegenüber direkt nach dem Tod des Erblassers tätig werden, aber die Erben können ihm die Vollmacht entziehen, sodass er nicht weiter tätig werden darf. Man kann aber beide Möglichkeiten kombinieren.

» Er kann daneben bereits zu Lebzeiten einen Vorsorgebevollmächtigten einsetzen, der ihn bei der Verwaltung seiner digitalen Angelegenheiten unterstützt.

» Es ist jedoch immer empfehlenswert, dass der Verbraucher seinem Vorsorgebevollmächtigten bzw. seinen Erben die Zugangsdaten zu seinen digitalen Inhalten zur Verfügung stellt. Hierbei kann er sich einer sogenannten digitalen Vorsorgeurkunde bedienen. Hierbei sichert der Vollmachtgeber die stets aktuell zu haltenden Zugangsdaten auf einem verschlüsselten lokalen Datenträger (z. B. einem USB-Stick). Zur Speicherung der Zugangsdaten empfiehlt sich die Verwendung

des Programms KeePass. Dieser Datenträger ist mit einem Masterpasswort gesichert, das bei einer Vertrauensperson, beispielsweise einem Notar, hinterlegt ist.

» Trotzdem müssen die Erben bzw. Stellvertreter des Erblassers aber im Rechtsverkehr noch beweisen, dass sie berechtigt sind, auf die Daten des Verbrauchers zuzugreifen. Dies können die Erben durch Vorlage eines eröffneten Testaments oder – wenn ein solches nicht vorliegt – eines Erbscheins tun. Ein Vorsorgebevollmächtigter kann die Vollmachtsurkunde vorlegen. Nach hier vertretener Auffassung reicht meist die Vorlage einer Kopie dieser Urkunden, insbesondere dann, wenn es sich lediglich um Nutzerkonten handelt, mit denen keine oder nur geringe finanzielle Interessen verbunden sind.

» Die Erben bzw. Bevollmächtigten müssen auch ihre Identität nachweisen, wenn der Dienstanbieter dies verlangt. Da die persönliche Vorlage von Ausweisen sehr kompliziert sein kann, ist grundsätzlich die Vorlage einer Ausweiskopie möglich. Allerdings hat der Verbraucher in diesem Fall das Recht, bestimmte Angaben im Ausweis (zumeist alles außer Name, Foto und Geburtsdatum) zu schwärzen. Bietet ein Dienstanbieter diese Möglichkeiten an, ist auch der Identitätsnachweis über das Postident-Verfahren oder die Online-Ausweisfunktion denkbar.

7 Vertragliche Vorsorgemöglichkeiten

Dieses Kapitel untersucht,

- wie zwischen Dienstanbietern und Verbrauchern vertraglich eine Übertragung von Nutzerkonten auf Rechtsnachfolger oder ein Zugriff von Bevollmächtigten vereinbart werden kann;
- welche technisch-organisatorischen Möglichkeiten es gibt, die Zugangsdaten weiterzugeben und sich als Berechtigter gegenüber den Dienstanbietern zu identifizieren;
- wie der Tod des Erblassers gegenüber den Dienstanbietern nachgewiesen werden kann;
- wie der Eintritt der Hilfsbedürftigkeit nachgewiesen werden kann und ob dies erforderlich ist.

7.1 Motivation

Obwohl eine eigenständige Vorsorge durch den Nutzer im Wege erbrechtlicher Verfügungen oder durch Vorsorgevollmacht für den Verbraucher vielfältige Regelungsmöglichkeiten eröffnet, kann dies dennoch mit verschiedenen Folgeproblemen verbunden sein, die sich insbesondere im Rahmen der Durchsetzung der Verfügungen gegenüber den Online-Dienstanbietern stellen. Vor diesem Hintergrund ist es vorteilhaft für die Verbraucher, wenn Dienstanbieter entweder zu individuellen vertraglichen Vereinbarungen mit den Nutzern bereit sind oder vertraglich bestimmte Vorsorgemöglichkeiten zur Verfügung stellen. Die Dienstanbieter sind in diesem Fall frühzeitig in die Vorsorge eingebunden und können die Verbraucher unterstützen. Zudem ist zu erwarten, dass sich im Vorsorgefall bei Einbindung des Dienstanbieters weniger Rechtsstreitigkeiten ergeben. Die nachfolgend vorgeschlagenen Lösungen werden bedeutsam, wenn sich Daten des Verbrauchers auf dem Server eines Dienstanbieters befinden. Sind Daten demgegenüber auf lokalen Speichermedien oder eigenen Servern des Verbrauchers gesichert, bieten sich eher die in den Kapiteln 6.2 auf Seite 176 bis 6.5 auf Seite 192 beschriebenen Vorsorgemöglichkeiten an.

7.2 Rechtliche Vorsorgemöglichkeiten

Über den in Kapitel 4.2.2 auf Seite 106 unterbreiteten Vorschlag einer gesetzlichen Verpflichtung der Dienstanbieter hinaus, sind in diesem Kapitel die rechtlichen und technischen Möglichkeiten zu untersuchen, wie zwischen Dienstanbieter und Verbraucher der Übergang von oder eine Zugriffsmöglichkeit Dritter auf Nutzerkonten auf freiwilliger Basis vereinbart werden kann. Dabei sollen sowohl Regelungen behandelt werden, die den Fall des Versterbens als auch der Handlungsunfähigkeit des Nutzers betreffen. Entscheiden sich die Dienstanbieter, vertragliche Regelungen zuzulassen, ist zu empfehlen, dass beide Konstellationen berücksichtigt werden.

7.2.1 Vertragliche Gestaltungsmöglichkeiten für den Todesfall

Zunächst ist denkbar, dass zwischen Dienstanbieter und Nutzer individualvertraglich oder durch AGB eine Regelung darüber getroffen wird, was im Fall des Versterbens mit dem Vertragsverhältnis geschehen soll.

7.2.1.1 Vereinbarung der Löschung des Nutzerkontos

Im Rahmen der vertraglichen Beziehung ist es grundsätzlich möglich, dass der Erblasser dem Dienstanbieter gegenüber (bindend) erklärt, dass die Vertragsbeziehungen mit seinem Tod enden und die Daten gelöscht werden – und so der Zugriff der Erben verhindert wird.

Allerdings ist für die praktische Umsetzbarkeit dieser Möglichkeit wohl erforderlich,[1] dass der Dienstanbieter selbst eine solche Möglichkeit vorschlägt oder allgemein bereithält, da zumindest große Anbieter aufgrund des enormen Verwaltungsaufwands nicht mit jedem Nutzer individuell die Vertragsbedingungen aushandeln, sondern diese in allgemeingültiger Form geregelt werden. Ist der Dienstanbieter aber zu Gestaltungen bereit, kann eine solche Vereinbarung als Erteilung einer postmortalen Vollmacht oder einer postmortalen Weisung im Rahmen des Vertragsverhältnisses eingeordnet werden. Möglich ist auch die Vereinbarung einer auflösenden Bedingung gemäß §§ 158 II, 163 BGB, wenn im Todeszeitpunkt das Vertragsverhältnis mit der Folge der Löschung der Daten beendet werden soll.[2] Die Wirksamkeit einer solchen Vereinbarung in AGB ist zwar unter anderem unter dem Gesichtspunkt des Transparenzgebots gemäß § 307 I 2 BGB im Einzelfall zu untersuchen,[3] individualvertraglich sind derartige Vereinbarungen aber auch aus erbrechtlicher Sicht möglich, da das vertragliche Verhältnis immer so auf die Erben übergeht, wie es mit dem Dienstanbieter vereinbart ist.[4] Insofern ist die eigene privatautonome Entscheidung des Nutzers, was nach seinem Tod mit seinen Daten und Rechtsverhältnissen geschehen soll, von seiner Testierfreiheit gedeckt.

Ist eine Löschung von Daten vereinbart, ist der Dienstanbieter sowohl daran gehindert, diese an dritte Personen (Erben, Angehörige oder Stellvertreter) herauszugeben, als auch verpflichtet, die Inhalte von den eigenen Servern oder Speichermedien zu löschen. Die diesbezügliche Kontrolle und Durchsetzung steht grundsätzlich den Erben als Rechtsnachfolger des Erblassers zu. Verletzt der Dienstanbieter durch seine Handhabung der Daten das postmortale Persönlichkeitsrecht, sind auch die nächsten Angehörigen befugt, eine Unterlassungsklage zu erheben.[5]

7.2.1.2 Vertrag zugunsten Dritter auf den Todesfall

Zudem besteht grundsätzlich die Möglichkeit, dass – unter der Prämisse, dass der Dienstanbieter sich hinsichtlich einer derartigen Vereinbarung offen zeigt – der Nutzer gegenüber dem Dienstanbieter erklärt, dass ein Account oder Vertragsverhältnis im Fall des Todes einer bestimmten Person zufallen soll. Dies kann als Vertrag zugunsten Dritter auf den Todesfall im Sinne der §§ 2301 II, 328 BGB eingeordnet werden.[6] So können schuldrechtliche Vertragsansprüche im Todesfall außerhalb des Erbrechts auf eine andere Person übertragen werden, indem der Nutzer mit dem versprechenden Dienstanbieter vereinbart, dass im Fall des Todes des Nutzers eine begünstigte dritte Person das Recht erwirbt, unmittelbar vom versprechenden Dienstanbieter die Leistung – Zugang zum Account und/oder Nutzungsmöglichkeit – zu fordern. Dieses Deckungsverhältnis zwischen versprechendem Dienstanbieter und dem Nutzer als Versprechensempfänger ist ein Rechtsgeschäft unter Lebenden. Im Verhältnis zwischen dem Versprechensempfänger als Schenker zu der dritten beschenkten Person hat dies zwar dieselben Ziele und Wirkungen wie eine Verfügung von Todes wegen. Trotzdem erhält der Dritte die Leistung nicht aus dem Nachlass, sondern unmittelbar vom Versprechenden aufgrund

[1] *Herzog*, in: Kroiß u. a. (Hrsg.), Nachfolgerecht, Kap. 9 Rn. 81.
[2] *Kutscher*, Digitaler Nachlass, S. 157.
[3] Dazu ausführlich *Kutscher*, Digitaler Nachlass, S. 157 ff. und in Kapitel 7.2.1.3 auf der nächsten Seite.
[4] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 366.
[5] *Herzog/Pruns*, Digitaler Nachlass, S. 157.
[6] *Herzog/Pruns*, Digitaler Nachlass, S. 157.

des Deckungsverhältnisses. Insofern wendet die überwiegende Ansicht hier nicht die erbrechtlichen Formvorschriften an, sondern stellt hinsichtlich der Formbedürftigkeit auf das (in der Regel) formfreie Deckungsverhältnis ab.[7] Soweit eine Schenkung anzunehmen und daher die notarielle Form einzuhalten ist (§ 518 I BGB), wird ein Formmangel jedenfalls mit Bewirkung der Leistung im Sinne des § 518 II BGB geheilt. Schenkungsgegenstand ist im Rahmen dieser Verträge der unmittelbare Anspruch gegen den Versprechenden.[8] Somit tritt der Vollzug der Schenkung und damit die Heilung nach § 518 II BGB mit dem Tod des Nutzers durch Erwerb des unmittelbaren Forderungsrechts gegen den Dienstanbieter ein, vgl. § 331 I BGB.[9]

Ist das diesbezügliche (mit dem Tod des Schenkers wirksam gewordene) Angebot zum Vertragsschluss dem Dritten zugegangen, kann es auch von den Erben nicht mehr widerrufen werden.[10] Vor Zugang des Angebots steht den Erben allerdings ein Widerrufsrecht i. S. d. § 130 I 2 BGB zu, das der Erblasser auch nicht ausschließen kann.[11] So könnten die Erben verhindern, dass ein wirksamer Rechtsgrund im Valutaverhältnis zustande kommt.[12] Hat der Dritte im Fall des wirksamen Widerrufs die Leistung bereits erhalten, muss er diese nach den Regeln des Bereicherungsrechts wieder herausgeben. Dieses zufällige Ergebnis, dass die Wirksamkeit davon abhängt, ob die Erben schnell genug sind, den Vertrag vor Zugang des Angebots zu widerrufen, kann dadurch verhindert werden, dass der Nutzer dem Dritten das Vertragsangebot noch zu Lebzeiten unterbreitet. Hier wie dort muss der Dienstanbieter jedoch zustimmen.[13]

Auf diese Weise könnte also ein Online-Vertragsverhältnis – im vom Nutzer bestimmten Umfang – auf einen Dritten übertragen werden.

7.2.1.3 Umsetzung durch ein Optionsrecht für die Nutzer

Genauer zu beleuchten ist jedoch die Frage, wie dies umgesetzt werden kann. Es ist möglich, dass eine entsprechende Vereinbarung in dem Sinne individualvertraglich zwischen Nutzer und Dienstanbieter geschlossen wird, dass der Nutzer eigene Vorschläge hinsichtlich der Art und Weise der Übertragung des Nutzerkontos machen kann. Allerdings werden auch hier in der Regel die Dienstanbieter aufgrund des enormen Verwaltungsaufwands derartige individualvertragliche Regelungen mit jedem einzelnen Nutzer ablehnen. Die Dienstanbieter könnten jedoch entsprechende Auswahlmöglichkeiten für die Nutzer durch ein Formular vorhalten, wobei diese durch Setzen von Häkchen und Benennung von Nachfolgern oder Vertrauenspersonen selbst auswählen könnten, was im Vorsorgefall mit dem Nutzerkonto geschehen soll. Insoweit ist jedoch strittig, ob eine derartige Regelung als AGB einzustufen ist und ob diese wirksam wäre. Bisher ist auch nicht abschließend geklärt, wie eine entsprechende Ausgestaltung aussehen kann.[14]

[7] BGH, NJW 1964, 1124 (1125); *Kutscher*, Digitaler Nachlass, S. 152 f.
[8] BGH, NJW 1975, 382 (383).
[9] *Litzenburger*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 2301 Rn. 18.
[10] OLG Düsseldorf, NJW-RR 1996, 1329.
[11] *Litzenburger*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 2301 Rn. 19.
[12] BGH, NJW 1975, 382 (383 f.).
[13] *Kutscher*, Digitaler Nachlass, S. 155.
[14] Ein konkreter Formulierungsvorschlag wird in Kapitel 9.3.1 auf Seite 355 unterbreitet.

Hinsichtlich des Erbfalls sollte eine vertragliche Regelung jedenfalls verschiedene Möglichkeiten für den Verbraucher vorhalten, was nach seinem Tod mit dem Nutzerkonto geschehen soll. Insofern bieten sich die Regelungsalternativen an, die auch durch erbrechtliche Verfügungen in der Regel erreicht werden können. Zunächst müsste daher die Löschung des Nutzerkontos angeboten werden. Eine weitere Möglichkeit – zumindest für Social-Media-Accounts – könnte das Versetzen des Kontos in den Gedenkzustand sein. Zudem müsste eine Übertragung auf einen Rechtsnachfolger möglich sein. Diesbezüglich wäre eine Auswahlmöglichkeit zwischen einem reinen Einsichtsrecht und einem aktiven Nutzungsrecht sowie ein Feld vorzusehen, in dem der Verbraucher einen oder mehrere Begünstigte benennen kann. Daneben sind die Alternativen erforderlich, dass der Verbraucher gar keine Regelung für den Todesfall treffen oder die Entscheidung aufschieben möchte. Insofern soll der Verbraucher nicht gezwungen werden, sofort eine Regelung zu treffen. Diesbezüglich könnte die Situation der Erben jedoch zusätzlich dadurch erleichtert werden, dass vertraglich – allerdings an anderer Stelle – festgelegt wird, dass eine Kopie oder ein Scan des Testaments samt Eröffnungsbeschluss oder, falls ein solches nicht vorhanden ist, eines Erbscheins zum Nachweis der Erbenstellung ausreichend ist, und indem die zum Empfang des Nachweises zuständige Stelle benannt wird. Es ist auch eindeutig darauf hinzuweisen, dass die einmal getroffene Entscheidung keine absolute und endgültige ist, sondern nachträglich (beliebig oft) geändert werden kann.

Um den Verbraucher bei der Entscheidung zu unterstützen, sind leicht zugängliche Informationen darüber bereitzustellen, welche Rechtsfolgen durch die jeweilige Auswahl ausgelöst werden. Dazu gehört auch, dass der Verbraucher (in knapper Form) in der Klausel über die gesetzliche Ausgangslage, also die grundsätzliche Vererbbarkeit von Online-Vertragsbeziehungen, informiert wird.

Zu bestimmen ist auch der den Eintritt des Vorsorgefalls bestimmende Umstand. Denkbar wäre, dass an die Inaktivität des Nutzers über einen gewissen Zeitraum angeknüpft wird. Dies ist jedoch ein relativ unsicherer Faktor, da es auch denkbar ist, dass Nutzerkonten aus freier Entscheidung über einen gewissen Zeitraum nicht genutzt werden. Zudem ist die Notwendigkeit des Ablaufs eines Zeitintervalls dann ungünstig, wenn zeitnah nach dem Tod des Nutzers der Rechtsnachfolger eintreten oder das Konto gelöscht werden soll. Der Nachweis über den Eintritt des Vorsorgefalls könnte daher durch die Vorlage der Kopie der Sterbeurkunde des Nutzers erbracht werden. Insofern wären auch hinsichtlich der Löschungs- und Gedenkzustandsoption Vertrauenspersonen zu benennen, die den Dienstanbieter über den Todesfall benachrichtigen.
Zwar erfahren die benannten Personen unter diesen Voraussetzungen bereits vor dem Todesfall von ihrer Begünstigung und damit gegebenenfalls auch von dem Umstand, dass die Entscheidung wieder geändert wird, was möglicherweise zu Konflikten führen kann. Im Gegensatz hierzu wäre dies bei einer Erbeinsetzung nicht zwingend der Fall. Wird der Nutzer allerdings darauf hingewiesen, kann er das diesbezügliche Risiko selbst einschätzen und entscheiden, wie er vorgehen möchte. Darüber hinaus ist die vertragliche Regelung nicht zwingend, der Nutzer kann auch entscheiden, dass die erbrechtlichen Regeln gelten sollen.
Alternativ könnte jedenfalls die Löschung dann erfolgen, wenn die Erben den Todesfall gegenüber dem Dienstanbieter anzeigen. Die Erben wären dann über die vertragliche Vereinbarung zu informieren; und anschließend wäre die Löschung des Kontos durch den Dienstanbieter vorzunehmen. Als Absicherung könnte zusätzlich vorgesehen werden, dass der Vorsorgefall bei Inaktivität über einen

langen Zeitraum (wohl 1–2 Jahre) vermutet wird. Diesbezüglich ist in der vertraglichen Regelung aber vorzusehen, dass der Nutzer vor der Löschung gewarnt wird.

Die vertraglichen Regelungen sind aber im Einzelfall an die Bedürfnisse des jeweiligen Vertragsverhältnisses anzupassen. So können die Dienstanbieter auch zusätzliche Einstellungen oder bestimmte Regelungen gerade nicht vorsehen bzw. einen anderen Umstand für den Eintritt des Vorsorgefalls bestimmen. Die hier erarbeitete Lösung stellt insoweit nur einen Vorschlag dar.

Eine derartige Regelung wäre auch wirksam. Insofern liegen zwar nach einer Ansicht selbst bei einer Auswahlmöglichkeit des Verbrauchers immer AGB vor,[15] sodass die Regelung einer AGB-Kontrolle standhalten müsste.

Hinsichtlich der hier vorgeschlagenen Lösung könnte jedoch vertreten werden, dass es sich nicht um AGB handelt, die durch die Dienstanbieter „gestellt“ werden, § 305 I 1 BGB, sondern um ausgehandelte Vertragsbedingungen, auch wenn dieses Merkmal zu Recht sehr streng ausgelegt wird. Zwar werden die Auswahlmöglichkeiten durch den Dienstanbieter vorformuliert. Auch solche vorformulierten Vertragsbedingungen können aber dann als ausgehandelt eingeordnet werden, „wenn sie der Verwender als eine von mehreren Alternativen anbietet, zwischen denen der Vertragspartner die Wahl hat.“ In diesem Fall darf die Vertragsbedingung nicht nur unselbstständiger Art sein, wie im Rahmen des Anfügens von Namen, sondern muss den Regelungsgehalt beeinflussen. Zudem darf der Verwender die Wahlfreiheit nicht durch die Gestaltung des Formulars oder in anderer Weise beeinflussen.[16]
Hier werden die Vorsorgemöglichkeiten dem Verbraucher als echte Alternativen zur Verfügung gestellt. Er kann selbst nach freier Wahl entscheiden, was nach seinem Tod mit dem Nutzerkonto geschehen soll. Zudem steht es dem Nutzer offen, ob er eine Regelung treffen möchte oder nicht, und zu welchem Zeitpunkt dies geschehen soll. Insofern wird ihre Verwendung nicht zum Abschluss des Vertrages verlangt. Die Einbeziehung ist vielmehr eine freie Entscheidung des Nutzers[17] und die Auswahl kann nachträglich wieder geändert werden, sodass das Merkmal des „Aushandelns“ bejaht werden könnte.

Allerdings ist zu berücksichtigen, dass es sich um einen Vertrag zwischen einem Dienstanbieter und einem Verbraucher handelt. Daher gelten gemäß § 310 III Nr. 1 BGB die AGB als vom Unternehmer gestellt, es sei denn, dass sie durch den Verbraucher in den Vertrag eingeführt wurden. Diesbezüglich wurde auch entschieden, dass es gerade nicht ausreichend ist, wenn der Verbraucher „lediglich die Wahl zwischen bestimmten, von der anderen Seite vorgegebenen Formularalternativen hat.“[18] Notwendig wäre demgegenüber, dass der Verbraucher die Möglichkeit hat, „alternativ eigene Textvorschläge mit der effektiven Möglichkeit ihrer Durchsetzung in die Verhandlungen einzubringen.“ Da die Dienstanbieter jedoch in der Regel eine solche Möglichkeit nicht zur Verfügung stellen, sondern nur die Auswahl zwischen den von ihnen vorgeschlagenen Alternativen besteht, liegen nach dieser Beurteilung AGB vor.

[15] Vgl. hierzu *Kutscher*, Digitaler Nachlass, S. 151 f.; *Litzenburger*, FD-ErbR 2018, 407688.
[16] BGH, NJW 2003, 1313 (1314).
[17] BGH, NJW 2016, 1230 (1231).
[18] Dazu und zum folgenden BGH, NJW 2010, 1131 (1133).

Auch wenn die Regelung als AGB eingestuft wird, ist die Wirksamkeit aber zu bejahen.
Dies gilt insbesondere dann, wenn die Regelung so ausgestaltet ist, dass sie dem Transparenzgebot (§ 307 I 2 BGB) genügt. Danach sind die AGB verständlich, klar und übersichtlich zu gestalten. Zunächst ist der Klauselinhalt daher möglichst eindeutig und nachvollziehbar darzustellen sowie zu konkretisieren, damit der Verbraucher seine Rechte und Pflichten dem Vertragstext mit größtmöglicher Bestimmtheit entnehmen kann (Bestimmtheitsgebot). Auch soll der Verbraucher „ohne fremde Hilfe möglichst klar und einfach seine Rechte feststellen können". Dem Verwender dürfen keine ungerechtfertigten Beurteilungsspielräume entstehen.[19] Insofern ist hinsichtlich der Formulierung der Klauseln darauf zu achten, dass keine Begriffe verwendet werden, die ungenau oder dem Verbraucher nicht vertraut sind.[20] Maßstab für die Transparenz sind die Verständnismöglichkeiten eines durchschnittlichen Vertreters des angesprochenen Kundenkreises. Werden – wie hier – die AGB somit im Massenverkehr gegenüber jedermann verwendet, richtet sich die Beurteilung der Verständlichkeit nach der Sicht eines durchschnittlich informierten (rechtsunkundigen) Bürgers.[21] Hierfür ist erforderlich, dass den Verbrauchern hinreichend deutlich vor Augen geführt wird, welche Rechtsfolgen durch die jeweilige Auswahl ausgelöst werden und welche Reichweite die Entscheidung hat.

Die vorgeschlagene Regelung stellt auch keine unzulässige Beschränkung des Erbrechts des Verbrauchers dar. Insoweit kommt es auf den Streit, ob diese Frage unter § 307 II Nr. 1 BGB (mit wesentlichen Grundsätzen des BGB, insbesondere § 1922 BGB, nicht vereinbar) oder unter § 307 I 1 BGB (unangemessene Benachteiligung entgegen den Geboten von Treu und Glauben) zu subsumieren ist, nicht an, da Beurteilungsmaßstab nach beiden Ansichten die unzulässige Beschränkung der Testierfreiheit nach Art. 14 GG ist.[22]

Eine solche liegt hier jedoch gerade nicht vor. Dies wäre nur zu bejahen, wenn dem Nutzer durch die AGB des Online-Dienstanbieters die Wahl genommen wird, zu entscheiden, wie nach seinem Tod mit den eigenen Daten zu verfahren ist. Hier hat der Verbraucher aber gerade die Möglichkeit, eine freie Entscheidung darüber zu treffen, ob beispielsweise eine Löschung oder Weitergabe der Online-Vertragsbeziehung und damit der Daten erfolgen soll. Die Auswahl wird dem Verbraucher somit nicht durch den Dienstanbieter aufgezwungen, sondern entspricht gerade dem Willen des Erblassers. Dies wird auch dadurch verstärkt, dass durch die Auswahlmöglichkeiten weitgehend die auch durch erbrechtliche Verfügungen möglichen Regelungsalternativen abgebildet werden. Insoweit könnte gerade ein Vorteil dieser Regelung darin gesehen werden, dass dem Verbraucher die ihm zur Verfügung stehenden Möglichkeiten vor Augen geführt werden. Das Schicksal der Daten nach dem Tod des Erblassers deckt sich somit mit seiner freien privatautonomen Entscheidung. Die erbrechtlichen Regelungen stehen dem hier nicht entgegen, vor allem, da es die freie Entscheidung des Erblassers ist, was nach seinem Tod zum Nachlass gehört.

Grundsätzlich ist es hierbei auch möglich, dass der Dienstanbieter dem Verbraucher weniger Regelungsalternativen zur Verfügung stellt, als hier vorgeschlagen werden. Erfolgt aber eine vertragliche

[19] Insgesamt hierzu BGH, NJW 2004, 1598 (1600).
[20] *Wurmnest*, in: Säcker u. a. (Hrsg.), MükoBGB, § 307 Rn. 62.
[21] *Wurmnest*, in: Säcker u. a. (Hrsg.), MükoBGB, § 307 Rn. 64.
[22] Vgl. zu erstgenannter Ansicht statt aller *Willems*, ZfPW 2016, S. 494 (509); zur a.A. statt aller *Lieder/Berneith*, FamRZ 2018, S. 1486 (1488).

Regelung, ist es zur Wirksamkeit der Vereinbarung jedenfalls erforderlich, dass eine Möglichkeit zur Löschung, zur Weitergabe des Nutzerkontos und zum Verzicht auf eine Regelung gegeben ist.

7.2.2 Vertragliche Gestaltungsmöglichkeiten für den Fall der Handlungsunfähigkeit

Auch hinsichtlich des Falls der Handlungsunfähigkeit könnte eine vertragliche Regelung zwischen Nutzer und Dienstanbieter dahingehend geschlossen werden, was bei Eintritt des Vorsorgefalls mit dem Nutzerkonto geschehen soll.

7.2.2.1 Vereinbarung der Löschung des Nutzerkontos

Die vertragliche Beziehung kann durch Erklärung des Verbrauchers gegenüber dem Dienstanbieter dergestalt ausgestaltet werden, dass im Fall des Eintritts der Handlungsunfähigkeit die Vertragsbeziehung enden und die mit dem Vertrag verbundenen Daten gelöscht werden sollen. Niemand wäre dann befugt, auf das Konto zuzugreifen. Eine solche Vereinbarung kann als Erteilung einer Vollmacht des Nutzers an den Dienstanbieter oder eine Weisung zur Löschung des Nutzerkontos eingestuft werden. Wie im Rahmen der Regelungen im Erbfall kann auch die Handlungsunfähigkeit die den Vertrag auflösende Bedingung i. S. d. §§ 158 II, 163 BGB darstellen. Solange der Nutzer noch handlungsfähig ist, kann er privatautonom bestimmen, dass mit dem Eintritt seiner Handlungsunfähigkeit auch die Vertragsbeziehung enden soll. Dies bietet sich insbesondere an, wenn mit dem Vertragsverhältnis private Daten verbunden sind und der Nutzer verhindern möchte, dass irgendeine dritte Person diese einsehen kann. Diesbezüglich ist der Fall zu bedenken, dass bei Fehlen einer Vorsorgevollmacht gerichtlich ein – dem Verbraucher persönlich unbekannter – Betreuer bestellt werden kann, der unter Umständen auf die Daten Zugriff nehmen könnte.

Auch in diesem Fall ist der Dienstanbieter daran gehindert, die Daten an einen Stellvertreter herauszugeben und verpflichtet, die Inhalte von seinen eigenen Servern und Speichermedien zu löschen.[23]

Im Rahmen der praktischen Umsetzbarkeit ist jedoch zu beachten, dass der Dienstanbieter in diesem Fall zuverlässig vom Eintritt der Handlungsunfähigkeit erfahren muss.

7.2.2.2 Benennung eines Stellvertreters gegenüber dem Dienstanbieter

Gegenüber dem Dienstanbieter kann auch eine Person benannt werden, die im Fall der Handlungsunfähigkeit auf das Nutzerkonto zugreifen und dieses verwalten können soll.

Diese Vertrauensperson würde insofern als Stellvertreter des Nutzers tätig. Grundsätzlich ist Stellvertreterhandeln stets zulässig und möglich, außer durch Rechtsgeschäft oder Gesetz ist dieses Recht

[23] Siehe hierzu auch bereits im Rahmen der vertraglichen Regelungen zum Erbfall.

ausgeschlossen. Wie in Kapitel 3 auf Seite 53 bereits festgestellt wurde, können sich Verbraucher auch im Rahmen von Online-Vertragsverhältnissen eines Stellvertreters bedienen. Dabei kann es hinsichtlich des Tätigwerdens des Bevollmächtigten vorteilhaft sein, wenn dem Dienstanbieter die Bevollmächtigung bereits vor Eintritt des Vorsorgefalls bekannt ist.

Die Benennung des Stellvertreters gegenüber dem Dienstanbieter kann insoweit entweder als Erteilung der Vollmacht durch Erklärung gegenüber einem Dritten, § 167 I Alt. 2 BGB, oder als Kundgabe der Vollmacht durch besondere Mitteilung an einen Dritten gemäß § 171 I Alt. 1 BGB eingestuft werden.

Die Benennung einer Vertrauensperson gegenüber dem Dienstanbieter könnte dabei i. S. d. § 167 BGB die Erteilung der Vollmacht selbst darstellen. Dadurch wird dem Bevollmächtigten die Rechtsmacht verliehen, im Namen des Vollmachtgebers für und gegen ihn Rechtsfolgen herbeizuführen. Ist der Dienstanbieter als Dritter Empfänger der Mitteilung, ist diese insofern Wirksamkeitsvoraussetzung für das Vertretergeschäft. Dadurch ist allerdings nur die Vollmachtserteilung und das rechtliche Können des Vertreters im Außenverhältnis festgelegt. Daneben muss in der Regel ein wirksames Grundverhältnis zwischen Stellvertreter und Vollmachtgeber bestehen.[24] Insofern wäre auch denkbar, dass der Bevollmächtigte gegenüber dem Dienstanbieter nicht ausdrücklich als Bevollmächtigter bezeichnet wird, sondern die Vollmachtserteilung konkludent durch schlüssiges Verhalten erfolgt, indem dem Stellvertreter Aufgaben übertragen werden, deren ordnungsgemäße Erfüllung eine Vollmacht erfordert.[25]

Die Benennung des Bevollmächtigten gegenüber dem Dienstanbieter könnte auch als Kundgabe der Vollmacht gegenüber einem Dritten i. S. d. 171 I BGB angesehen werden (kundgegebene Innenvollmacht). Die Kundgabe selbst hat dabei in der Regel nur deklaratorischen Charakter und ist von der ursprünglichen Vollmachtserteilung gegenüber dem Vertreter zu unterscheiden. Sie ist insofern unabhängig davon, ob im Innenverhältnis tatsächlich eine Vollmacht besteht, und begründet nur einen Rechtsscheintatbestand über das Bestehen der Innenvollmacht.[26] Der Dritte darf nach der Kundgabe somit auf das Bestehen der Vollmacht vertrauen. Die Vertretungsmacht bleibt ihm gegenüber bestehen, bis die Kundgebung in derselben Weise, wie sie erfolgt ist, widerrufen wird, § 171 II BGB. Ist die Innenvollmacht aber vollumfänglich wirksam, hat der Rechtsscheintatbestand keine eigenständige Bedeutung.[27]

Auch durch die Erteilung der Vollmacht gegenüber einem Dritten i. S. d. 167 I BGB wird zugleich ein Rechtsscheintatbestand über das Bestehen der Vollmacht gesetzt, der über den Bestand der Vollmacht hinaus Wirkung entfaltet. Im Einzelfall kann dies daher auch die Kundgabe einer bereits erteilten Innenvollmacht (§ 171 BGB) darstellen.[28] Demgegenüber stellt die Kundgabe gemäß § 171 I BGB zwar regelmäßig keine Erteilung einer Außenvollmacht dar.[29] Etwas anderes gilt aber, wenn

[24] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 1 f.
[25] *Schäfer*, in: Bamberger u. a. (Hrsg.), BeckOK BGB, § 167 Rn. 7.
[26] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 171 Rn. 1 f.
[27] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 171 Rn. 14.
[28] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 12.
[29] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 171 Rn. 1 f.

durch die Erklärung im Rechtsverkehr der Eindruck hervorgerufen wird, dass es sich um eine eigenständige Bevollmächtigung und nicht lediglich um eine Kundgabe handelt.[30] Insofern können die Übergänge fließend sein.

Bedeutsam ist, dass jedenfalls die Vollmacht dem Dienstanbieter als dritter Person mitgeteilt wurde, wodurch der Rechtsschein der Bevollmächtigung besteht. Sie muss daher gemäß den Erfordernissen der §§ 170 f. BGB gegenüber dem Dienstanbieter ausdrücklich widerrufen werden, wenn der Stellvertreter nicht mehr wirksam gegenüber dem Dienstanbieter tätig werden können soll.

Grundsätzlich ist die Vollmachtserteilung als einseitige empfangsbedürftige Willenserklärung auch unabhängig von der Annahme des Bevollmächtigten. Insbesondere wenn die Vollmacht aber durch Erklärung gegenüber einem Dritten erteilt wurde, ist zu empfehlen, dass Einverständnis zwischen dem Bevollmächtigten und dem Vollmachtgeber über das Bestehen der Vollmacht und die Befugnisse aus dem Grundverhältnis besteht. Dies gilt umso mehr im Rahmen der Kundgabe der Vollmacht, da hier der Rechtsschein regelmäßig unabhängig von der Bevollmächtigung eintritt. Der Verbraucher sollte daher mit der gegenüber dem Dienstanbieter benannten Person abklären, ob diese bereit ist, im Fall der Handlungsunfähigkeit das Konto zu verwalten und gegebenenfalls konkrete Anweisungen hinsichtlich der Durchführung der Verwaltung erteilen, damit der Wille des Verbrauchers im Vorsorgefall auch zur Geltung kommen kann. Dies gilt auch vor dem Hintergrund, dass der Bevollmächtigte zur Wahrung seiner Privatautonomie berechtigt ist, die Vollmacht gemäß § 333 BGB analog zurückzuweisen oder auf diese zu verzichten.[31]

7.2.2.3 Umsetzung durch ein Optionsrecht für die Nutzer

Auch für den Fall der Handlungsunfähigkeit ist zu untersuchen, wie eine entsprechende vertragliche Regelung umgesetzt werden kann. Erneut empfiehlt es sich, dass der Dienstanbieter Auswahlmöglichkeiten für den Nutzer zur Verfügung stellt, die es dem Verbraucher durch Setzen von Häkchen und Benennung von Vertrauenspersonen ermöglicht zu entscheiden, was im Fall der Handlungsunfähigkeit mit dem Nutzerkonto geschehen soll.[32]

Auch hier wären verschiedene Auswahlmöglichkeiten für die Verbraucher vorzusehen. Eine solche Regelung sollte die Möglichkeit der Löschung des Nutzerkontos vorsehen. Daneben sind die Regelungsalternativen darauf zu erstrecken, dass ein Stellvertreter gegenüber dem Dienstanbieter tätig werden kann. Insofern könnte eine weitere Unterscheidung danach erfolgen, ob der Stellvertreter lediglich ein Einsichtsrecht haben soll oder ein umfassendes Verwaltungsrecht. Zudem wäre ein Textfeld vorzusehen, in dem der Nutzer den Stellvertreter benennen kann. Dem Verbraucher muss jedoch auch die Möglichkeit offenstehen, auszuwählen, dass er gar keine Regelung für den Fall der Handlungsunfähigkeit treffen oder die Entscheidung aufschieben möchte. In diesem Zusammenhang ist jedoch darauf hinzuweisen, dass möglicherweise durch den Nutzer vorgenommene Handlungen nicht mehr anerkannt werden, wenn bei dem Dienstanbieter der begründete Verdacht besteht, dass

[30] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 11.
[31] *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 5.
[32] Ein konkreter Formulierungsvorschlag wird in Kapitel 9.3.2 auf Seite 358 unterbreitet.

der Nutzer nicht mehr handlungsfähig ist. Zusätzlich ist klarzustellen, dass in diesem Fall auch ein dem Dienstanbieter unbekannter Stellvertreter gegenüber diesem tätig werden kann, wenn er seine Bevollmächtigung nachweist. Um eine weitere Erleichterung für die Verbraucher zu schaffen, könnte an anderer Stelle festgelegt werden, welche Anforderungen an diesen Nachweis zu stellen sind. Beispielsweise könnte eine Kopie oder ein Scan von Vollmachtsurkunde oder Betreuerausweis als ausreichender Nachweis bestimmt werden.
Zudem muss ein klarstellender Hinweis erfolgen, dass die einmal getroffene Entscheidung weder absolut noch endgültig und eine nachträgliche Änderung möglich ist.

Darüber hinaus ist der Verbraucher darüber zu informieren, welche Rechtsfolgen und Rechtswirkungen durch die getroffene Auswahl ausgelöst werden.

Lediglich hinsichtlich der Löschung ist zudem der den Eintritt des Vorsorgefalls bestimmende Umstand festzulegen. Eine Bevollmächtigung sollte nicht vom Eintritt der Handlungsunfähigkeit abhängig gemacht werden.[33]

Hinsichtlich der Differenzierung von Einsichts- und Verwaltungsrecht im Rahmen der Stellvertretung wäre es grundsätzlich sinnvoll, wenn dem Stellvertreter – zumindest wenn ihm nur ein Einsichtsrecht zusteht – ein eigener Satz Zugangsdaten zur Verfügung gestellt wird. Der Zugang des Stellvertreters könnte dann so konfiguriert sein, dass nur die zur Einsicht erforderlichen Funktionen freigeschaltet sind. Ist dies technisch nicht möglich, wäre die diesbezügliche Differenzierung gegenüber dem Dienstanbieter wohl obsolet. Verwenden Vollmachtgeber und Stellvertreter denselben Zugang, müsste zudem vertraglich geregelt werden, wie der Stellvertreter die Zugangsdaten erhält. Insofern könnte entweder dem Nutzer selbst auferlegt werden, diese an den Stellvertreter weiterzugeben, oder der Dienstanbieter könnte diese zur Verfügung stellen, wenn der Stellvertreter Zugriff auf das Konto begehrt.

Sinnvoll ist es auch, dass der Dienstanbieter den Bevollmächtigten nach Benennung durch den Nutzer benachrichtigt und ihm die Folgen der Erklärung des Nutzers für ihn mitteilt. Dies gilt vor dem Hintergrund, dass zwar die Vollmachtserteilung nicht von der Annahme durch den Bevollmächtigten abhängt, dieser aber das Recht hat, die Stellvertretung zurückzuweisen. Weist der Stellvertreter die Aufgabe zurück, wäre der Nutzer gegebenenfalls durch den Dienstanbieter zu benachrichtigen. So kann einerseits abgeklärt werden, ob tatsächlich eine wirksame Stellvertretung vorliegt, und dass – nach dem Willen des Verbrauchers – im Vorsorgefall die benannte Person auch tatsächlich tätig wird.

Die vertraglichen Regelungen sind aber im Einzelfall an die Bedürfnisse des jeweiligen Vertragsverhältnisses anzupassen. So können die Dienstanbieter auch zusätzliche Einstellungen oder bestimmte Regelungen gerade nicht vorsehen bzw. einen anderen Umstand für den Eintritt des Vorsorgefalls bestimmen. Die hier erarbeitete Lösung stellt insoweit nur einen Vorschlag dar.

Auch hier wäre eine entsprechende Regelung unabhängig davon wirksam, ob es sich um AGB oder eine individualvertragliche Regelung handelt. Hinsichtlich dieses Streits kann auf die Ausführungen in Kapitel 7.2.1.3 auf Seite 294 verwiesen werden.

[33] Zu Begründung und Auswirkungen siehe ausführlich Kapitel 7.5 auf Seite 330

Unter der Prämisse, dass es sich auch hier um AGB handelt, ist deren Wirksamkeit jedoch anhand der vorliegenden Konstellation zu bestimmen.

Das Formular zur Benennung eines Stellvertreters ist so zu formulieren, dass dies lediglich ein Angebot darstellt. Es ist darauf hinzuweisen, dass ein Stellvertreter auch dann gegenüber dem Dienstanbieter tätig werden kann, wenn er nicht im Vorfeld gegenüber dem Dienstanbieter benannt wurde. Es würde eine nach § 309 Nr. 13c BGB unwirksame Klausel vorliegen, wenn die Anzeige oder Erklärung der Bevollmächtigung an besondere Zugangserfordernisse gebunden würde. Dies wäre der Fall, wenn die einzige Möglichkeit, einen Stellvertreter zu benennen, durch das von dem Dienstanbieter zur Verfügung gestellte Formular erfolgen könnte, und nicht auch durch Vorlage der Vollmachtsurkunde durch den Stellvertreter. In diesem Fall würden an den Zugang strengere Anforderungen als nach § 130 BGB geknüpft, da es danach ausreicht, wenn die Anzeige oder Erklärung in *verkehrsüblicher Weise* in die tatsächliche Verfügungsgewalt des Verwenders gelangt.[34] In verkehrsüblicher Weise kann die Mitteilung einer Bevollmächtigung aber auch durch Vorlage der Vollmachtsurkunde oder im Fall der Betreuung durch Vorlage des Betreuerausweises erfolgen. Diese Möglichkeit darf daher durch die vertragliche Regelung nicht ausgeschlossen werden.

Daneben darf die Klausel auch nicht so zu verstehen sein, dass Vollmachten generell gegenüber den Dienstanbietern im Vorfeld angezeigt werden müssen. Dies würde jedenfalls eine unangemessene Benachteiligung i. S. d. § 307 I 1 BGB darstellen. Gerade wenn die Vollmacht nach der Intention des Verbrauchers als Vorsorgevollmacht für den Fall seiner Handlungsunfähigkeit erteilt wurde, könnte eine gegebenenfalls versäumte Anzeige gegenüber den Dienstanbietern im Vorsorgefall aufgrund einer fehlenden Geschäftsfähigkeit auch nicht mehr nachgeholt werden.[35] Ein Stellvertreter könnte somit im Fall der Handlungsunfähigkeit trotz Bestehens einer wirksamen Bevollmächtigung nicht gegenüber dem Dienstanbieter tätig werden, sodass bei Vorliegen der weiteren Voraussetzungen – entgegen des ausdrücklichen Willens des Verbrauchers – gerichtlich ein Betreuer zu bestellen wäre. Die vertragliche Regelung könnte somit dazu führen, dass die Wirksamkeit der Vorsorgevollmacht ausgehöhlt wird.

Darüber hinaus muss die vertragliche Regelung dem Transparenzgebot i. S. d. § 307 I 2 BGB genügen. Nach den in Kapitel 7.2.1.3 auf Seite 294 herausgearbeiteten Anforderungen ist auch hier der Vertragstext so verständlich, klar und übersichtlich zu gestalten, dass für den Verbraucher deutlich wird, welche Rechtsfolgen und Rechtswirkungen durch die jeweilige Auswahl ausgelöst werden.

Grundsätzlich ist auch darauf hinzuweisen, dass die einmal getroffene Entscheidung – insbesondere die Benennung eines Stellvertreters – gegenüber dem Dienstanbieter nicht endgültig ist, sondern (beliebig oft) geändert werden kann. Hat der Verbraucher bereits einen Stellvertreter gegenüber dem Dienstanbieter benannt und möchte er dessen Vertretungsmacht widerrufen, muss er dies dem Dienstanbieter mitteilen, da sonst ein Rechtsscheintatbestand (§§ 170 f. BGB) für das Weiterbestehen der Vollmacht gegenüber dem Dienstanbieter besteht. Der nicht mehr wirksam Bevollmächtigte könnte somit weiter Rechtshandlungen für den Stellvertreter vornehmen. Für die diesbezügliche Mitteilung ist es aber ausreichend, wenn der Verbraucher die in dem Formular getroffene Auswahl ändert

[34] *Wurmnest*, in: Säcker u. a. (Hrsg.), MükoBGB, § 309 Nr. 13 Rn. 10.
[35] Diesbezüglich im Rahmen des Bankrechts: *Schubert*, in: Säcker u. a. (Hrsg.), MükoBGB, § 167 Rn. 78.

und dies in den Einstellungen speichert. Auf diese Weise kann der Dienstanbieter Kenntnis davon nehmen, dass die Stellvertretung durch die nun nicht mehr benannte Person nicht mehr gewünscht ist.

Dem Dienstanbieter steht es frei, eine Regelung zu treffen, die dem Verbraucher weniger Alternativen zur Verfügung stellt. Wird aber die Benennung eines Stellvertreters gegenüber dem Dienstanbieter vorgesehen, ist zur Wirksamkeit der Vereinbarung zwingend erforderlich, dass die Möglichkeit eröffnet wird, auf eine vertragliche Regelung mit dem Dienstanbieter zu verzichten und auf andere Weise einen Stellvertreter zu benennen, der gegenüber dem Dienstanbieter Handlungen für den Nutzer vornehmen kann.

7.3 Technisch-organisatorische Umsetzung

Hier werden technische Verfahren dargestellt, die momentan im Rahmen der Weitergabe der Zugangsdaten diskutiert werden (Kapitel 7.3.1 und 7.3.2 auf Seite 305) und solche, die bisher bei der Identifikation diskutiert werden (Kapitel 7.3.3 auf Seite 309 bis 7.3.5 auf Seite 312). Insofern kann diese Darstellung nach der hier vertretenen Auffassung an dieser Stelle gemeinsam erfolgen.

7.3.1 Erweiterung der Passwort-Vergessen-Funktion

7.3.1.1 Technische Darstellung und Bewertung

Die Passwort-Vergessen-Funktion wurde bereits im Kapitel 6.5.2 auf Seite 195 dargestellt. Mögliche Erweiterungen dieser Funktion im Sinne des digitalen Nachlasses könnten Teil der vertraglichen Vereinbarungen zwischen Nutzer und Dienstanbieter werden. Zielführend wäre beispielsweise, wenn der Kontoinhaber die Passwort-Vergessen-Funktion zu Lebzeiten so konfigurieren könnte, dass bereits ein zweiter Satz Login-Daten (E-Mail-Adresse, Passwort) für eine Vertrauensperson im Konto angelegt werden kann. Diese zusätzlichen Login-Daten müssten zum Zeitpunkt des Vererbens – beispielsweise durch einen DeathSwitch (siehe Kapitel 7.4.1 auf Seite 317) – für die Vertrauensperson aktiviert werden. Auf diese Weise würde ein Konto direkt und auch für den Anbieter nachvollziehbar auf die Vertrauensperson übergehen. Die Dienste könnten jedenfalls jedem Kontoinhaber bereits bei der Erstregistrierung die Hinterlegung von Login-Daten eines oder mehrerer Vertreter nahelegen. Diese zusätzlichen Login-Daten würden dann auf Wunsch solange inaktiv bleiben, bis tatsächlich ein Notfall/Sterbefall des primären Kontoinhabers eingetreten ist. Die eindeutige Feststellung eines Sterbefalls ist für den Anbieter allerdings nicht trivial.

Auch wäre die folgende Erweiterung der Passwort-Vergessen-Funktion denkbar: Das Setzen einer neuen E-Mail-Adresse zusätzlich zum neuen Passwort, damit die Erben für den Zugriff auf das geerbte Konto nicht gezwungen sind, auf das E-Mail-Konto des Erblassers zuzugreifen (dessen Passwort sie evtl. nicht kennen). Dazu müssten auch die Antworten zu den ggf. vorgesehenen Sicherheitsabfragen neu gesetzt werden können, weil nicht davon ausgegangen werden kann, dass die

Erben die bisherigen Antworten kennen. Um damit keine neuen Angriffsmöglichkeiten zu schaffen, sollte dafür mindestens eine Zwei-Faktor-Authentisierung vorgeschrieben sein,[36] beispielsweise mittels Einsatzes eines U2F-Security-Token nach dem FIDO-Standard[37] oder die zusätzliche Eingabe eines Codes, der von einem TAN-Generator erzeugt wurde. Eine solche zusätzliche Authentisierung setzt natürlich die erfolgreiche Weitergabe des dafür notwendigen Geräts an die Erben voraus. Die zweite Authentisierung sollte in jedem Fall unter Einbindung eines zweiten, unabhängigen Kommunikationskanals erfolgen, d. h. es wäre sicherlich unzureichend, eine SMS an dasselbe Smartphone zu senden, auf dem der Nutzer auf die Passwort-Vergessen-Funktion geklickt hat.

Fazit: Eine Erweiterung der Passwort-Vergessen-Funktion um das sofortige Neusetzen der E-Mail-Adresse (Benutzername) und der Sicherheitsantworten zusätzlich zum neuen Passwort würde zusätzliche Sicherheitsmaßnahmen erfordern, z. B. die Präsentation eines Hardware-Tokens oder die Nutzung eines TAN-Generators. Dies würde aufseiten der Nutzer Kosten verursachen und die Kontoübergabe vom Erblasser auf den Erben komplizierter machen, da zusätzliche Geräte und Anweisungen an die Erben übergeben werden müssen.

7.3.1.2 Rechtliche Bewertung

Die Erweiterung der Passwort-Vergessen-Funktion um eine zusätzliche E-Mail-Adresse des Nachfolgers oder Stellvertreters wäre aus rechtlicher Sicht grundsätzlich sinnvoll. Dies bietet sich dann an, wenn vertraglich für den Todesfall ein Rechtsnachfolger oder Stellvertreter gegenüber dem Dienstanbieter benannt wurde. Für den Dienstanbieter wäre auf diese Weise erkennbar, wann der Übergang auf die Vertrauensperson stattgefunden hat.

Nach der in Kapitel 7.2 auf Seite 292 vorgeschlagenen Lösung soll der Nutzer auch danach differenzieren können, ob der Begünstigte lediglich ein Einsichts- und Zugriffsrecht oder ein vollständiges Nutzungsrecht des Kontos erhält. Insbesondere hinsichtlich des (insoweit beschränkten) Einsichtsrechts wäre auf diese Weise wohl möglich, dass der Zugang des Begünstigten von Anfang an so konfiguriert wird, dass nur die zur Einsichtnahme erforderlichen Funktionen freigeschaltet sind. Je nach Art der Online-Vertragsbeziehung könnten beispielsweise die Funktionen Nachrichten zu senden und Inhalte zu teilen (Social-Media-Konto) oder die Berechtigung, Zahlungsaufträge zu erteilen (Online-Bezahldienstkonto), gesperrt sein. Dies könnte im Todesfall dadurch erreicht werden, dass nach Mitteilung des Sterbefalls die Funktionen für das Konto insgesamt gesperrt werden. So könnte dem Willen des Nutzers Rechnung getragen werden.

Hinsichtlich des Erbfalls könnte es insoweit – auch aus Gesichtspunkten der Trauerbewältigung – sinnvoll sein, wenn den Erben entweder eigene Login-Daten zur Verfügung stehen oder sie zusätzlich zum neuen Passwort auch zeitgleich eine neue E-Mail-Adresse setzen könnten, um nicht über eine

[36] Mit der EU-Zahlungsdiensterichtlinie wird die Zwei-Faktor-Authentisierung seit 2018 für das Onlinebanking vorgeschrieben. Online-Dienstanbieter anderer Bereiche wie Amazon und Google bieten die Zwei-Faktor-Authentisierung als Option an und empfehlen deren Nutzung.

[37] U2F steht für „Universal Second Factor“ auf Grundlage einer Challenge-Response-Authentifizierung, FIDO für „Fast IDentity Online“, einem offenen und lizenzfreien Industriestandard für die weltweite Authentifizierung im Internet, siehe https://fidoalliance.org/how-fido-works.

längere Dauer die E-Mail-Adresse des Erblassers verwenden zu müssen. Durch die Anpassung der E-Mail-Adresse kann auch besser gewährleistet werden, dass die Erben nicht (private) Nutzerkonten des Erblassers unverändert weiternutzen. Insoweit könnte Missbrauchsfällen vorgebeugt werden. Aufgrund des Aufwands der zweiten Methode in Bezug auf eine Zwei-Faktor-Authentifizierung ist eher die erste Möglichkeit zu empfehlen, da diese aus rechtlicher Sicht ausreichend ist.

7.3.2 Erweiterte Konfigurationsmöglichkeiten der Dienste

7.3.2.1 Technische Darstellung und Bewertung

Keine der in Kapitel 6.5 auf Seite 192 genannten Verfahren zur Bereitstellung von Zugangsdaten bezieht systematisch und ausreichend die Online-Dienstanbieter mit in die Vorsorge ein. Sind die Online-Dienste nicht direkt in die Vorsorge einbezogen und darüber informiert, werden sie im Sterbefall möglicherweise von der Übernahme eines Kontos durch eine andere Person überrascht. Die Vertrauenspersonen des Verstorbenen können mit den empfangenen Zugriffsdaten zwar kurzfristig Erbrechtsprobleme und eine Auseinandersetzung mit Dienstanbietern umgehen, indem sie sich einfachen Zugang zu den Daten verschaffen. Sie können sich aber nicht sicher sein, dass die Übernahme eines Kontos überhaupt rechtmäßig ist und vom betreffenden Dienstanbieter akzeptiert wird.

Einige Quellen sprechen sich dafür aus, dass die Dienstanbieter systemeigene, dedizierte Funktionen zur Nachlassverwaltung anbieten (vgl. die im Kapitel 6.5.9.1 auf Seite 221 genannten drei Optionen), sodass die Nutzer ihren digitalen Nachlass direkt über den jeweiligen Online-Dienst regeln können, sich nicht um die Weitergabe von Zugriffsdaten und separate Anweisungen an die Erben kümmern müssen. Allerdings müsse dabei verhindert werden, dass die Erben das Konto uneingeschränkt im Namen des Erblassers weiterführen können, da dies nicht immer im Sinne des Erblassers wäre und zudem neue Angriffsmöglichkeiten für Identitätsmissbrauch schaffe.[38]

Systemeigene Funktionen der Online-Dienste könnten die Vorsorge und die Nachlassverwaltung tatsächlich stark vereinfachen. Dazu müssten die Dienstanbieter zumindest die wichtigsten Präferenzen ihrer Nutzer kennen und entsprechende Optionen anbieten. Nutzer müssten für jedes Konto individuell ihre Präferenzen für den digitalen Nachlass leicht festlegen und überprüfen können. Es sollte möglich sein, für die verschiedenen Daten (Daten der sozialen Netzwerke, Blogs, E-Mail, Foto-Alben etc.) einen unterschiedlichen Umgang im Nachlass festzulegen. Beispielsweise könnte für ein Online-Konto ein Gedenkzustand, in dem Freunde Kommentare hinterlassen können, erwünscht sein, während für ein E-Mail-Konto oder Blog vielleicht ein ausschließlich lesender Zugriff angemessen wäre.[39]

[38] *Kwoska*, Digitaler Nachlass – ein Aspekt der Techniksouveränität, in: Partizipative Technikentwicklung: Methodik und Umsetzungsbeispiele, S. 77.

[39] *Micklitz/Ortlieb/Staddon*, „I hereby leave my email to ...“: data usage control and the digital estate, in: 2013 IEEE Security and Privacy Workshops, S. 42–44.

Google bietet seit 2013 seinen Nutzern einfache Nachlassoptionen in Form des sogenannten „Kontoinaktivität-Managers“ an.[40] Damit können Nutzer selbstständig bei Google hinterlegen, welche Personen Zugriff auf die verschiedenen Google-Konten (z. B. Blogger, Google Drive, Gmail, Google Voice, YouTube) erhalten sollen, wenn die Konten über einen längeren Zeitraum (3 bis 12 Monate) nicht genutzt werden. Nach Ablauf des festgelegten Zeitraums wird dem Kontoinhaber eine Kontroll-SMS an die hinterlegte Telefonnummer gesendet. Reagiert der Kontoinhaber nicht, werden entsprechend der eingestellten Optionen sofort das Konto und dessen Inhalte gelöscht oder die vom Inhaber angegebenen Vertrauenspersonen benachrichtigt. Der Kontoinhaber kann zusätzlich hinterlegen, wer Zugriff auf die Konten bekommen soll. Aufgrund der vorliegenden Nutzereinstellungen braucht Google im Sterbefall keine Sterbeurkunden oder Erbscheine von den Erben anzufordern. Die Lösung kann als praktische Unterstützung der postmortalen Privatsphäre gesehen werden, orientiert sich aber nicht an den erbrechtlichen Vorschriften des BGB.[41]

Facebook bietet seinen Nutzern die einfache Option, eine Vertrauensperson als Nachlasskontakt („Facebook Legacy Contact“) einzurichten. Diese Person soll sich im Sterbefall um das Konto kümmern. Die Zugriffsrechte der Vertrauensperson sind allerdings auf das Verwalten des Kontos im Gedenkzustand beschränkt. Die Person kann sich eine Kopie der vom Kontoinhaber geteilten Inhalte (z. B. Fotos, Posts, Profilinformationen) herunterladen und das Konto löschen lassen, sich aber nicht anstelle des Kontoinhabers einloggen, um sich beispielsweise die privaten Einträge des Inhabers anzusehen. Zudem muss die Vertrauensperson selbst ein Facebook-Konto haben.[42] Die Facebook-Lösung ermöglicht es Nutzern, eine Vertrauensperson unter ihren Facebook-Freunden auszuwählen, ohne in dieser Frage auf Familienangehörige Rücksicht nehmen zu müssen. Damit begünstigt die Lösung die Kontoinhaber vor deren Familienangehörigen, die im Sterbefall evtl. ein weitergehendes Interesse an den Facebook-Seiten des Verstorbenen haben.[43]

Fazit: Die Konfigurationsmöglichkeiten einiger Online-Dienste wie Google und Facebook bieten ihren Nutzern verschiedene technische Optionen für den digitalen Nachlass. Dies hat einige Vorteile: Die Nutzer können selbstbestimmt vorsorgen und den Nachlass klar regeln, unter der Voraussetzung, dass der Dienst die Nutzerwünsche auch unterstützt. Im Sterbefall brauchen sich die Erben nicht um Sterbeurkunden oder Erbscheine zu kümmern. Solche Konfigurationsmöglichkeiten können die postmortale Privatsphäre praktisch unterstützen, schaffen allerdings Lösungen, die von den Dienstanbietern vorgeschrieben werden und damit weitgehend an die Interessen der Dienstanbieter gebunden sind.

[40] Google Kontoinaktivität-Manager, https://support.google.com/accounts/answer/3036546?hl=de.
[41] *Funk*, Das Erbe im Netz: Rechtslage und Praxis des digitalen Nachlasses, S. 35.
[42] Facebook: Was sind Nachlasskontakte und was können sie mit meinem Facebook-Konto tun? https://www.facebook.com/help/1568013990080948.
[43] *Harbinja*, Post-mortem privacy 2.0: theory, law, and technology. in: International Review of Law, Computers & Technology 31.1, S. 36 f.

7.3.2.2 Rechtliche Bewertung

Die Konfiguration der Dienste – soweit sie durch die Dienstanbieter vorgesehen ist – setzt eine vertragliche Regelung zur Übertragung von Nutzerkonten voraus. Dies ist – wie oben bereits beschrieben – grundsätzlich möglich. Durch die vertragliche Regelung können nicht nur Kontaktpersonen benannt werden, die dem Dienstanbieter einen Vorsorgefall mitteilen, sondern auch die Übertragung eines Nutzerkontos auf eine dritte Person kann im Wege der vertraglichen Regelung erfolgen. Eine erbrechtliche Verfügung ist hinsichtlich dieses Nutzerkontos daneben nicht unbedingt erforderlich. Vorteil ist insofern, dass der Dienstanbieter von Anfang an in die Vorsorge eingebunden ist und sich im Vorsorgefall weniger Probleme hinsichtlich der Legitimation der Begünstigten stellen. Soweit beispielsweise Google den Kontoinaktivität-Manager anbietet, hat dies daneben den Vorteil, dass es sich um eine systemeigene Lösung handelt, die nicht auf den Sterbefall begrenzt ist, sondern auch im Fall der Handlungsunfähigkeit Wirkung entfalten kann.

Soweit Anbieter die Konfiguration der Dienste jedoch überhaupt anbieten, wird die ständige Gefahr gesehen,[44] dass der Dienstanbieter seinen Dienst einstellt oder die Nutzungsbedingungen ändert. So sei denkbar, dass die Übertragungsmöglichkeiten ab einem bestimmten Zeitpunkt einfach nicht mehr angeboten werden und die Vorsorge somit hinfällig ist. Der Nutzer muss somit mindestens hinsichtlich der aktuellen Nutzungsbedingungen auf dem Laufenden bleiben. Die Änderung der Nutzungsbedingungen kann sich vor allem dann als problematisch darstellen, wenn der Nutzer zu diesem Zeitpunkt bereits geschäftsunfähig ist.

Dies ist jedoch eine Problematik, die sich generell im Rahmen der vertraglichen Vorsorge stellt. Hinsichtlich der Einstellung des Dienstes ist zu beachten, dass in diesem Fall auch das Konto des Verbrauchers nicht mehr existiert. In diesem Fall kann auch keine Übertragung mehr erfolgen – weder nach vertraglichen noch nach erbrechtlichen Regeln.

Zudem ist ein Dienstanbieter verpflichtet, die Nutzer auf eine Änderung von Vertragsbedingungen rechtzeitig und eindeutig hinzuweisen. In der Regel ist auch eine Zustimmung zu den geänderten Vertragsbedingungen erforderlich. Jedenfalls kann eine Änderung, die gegebenenfalls die Vorsorge des Verbrauchers beeinträchtigen würde, nicht ohne Kenntnis des Nutzers vollzogen werden. Der Nutzer hat somit die Möglichkeit, auf die Änderung zu reagieren und entweder seine vertragliche Vorsorge der neuen Situation anzupassen oder von dieser abzusehen und stattdessen eine testamentarische Verfügung zu verfassen.

Insgesamt ist hinsichtlich der Konfiguration der Dienste zu beachten, dass diese vertragliche Regelung mit dem Dienstanbieter stets individuell für jeden einzelnen Dienstanbieter einzurichten und an Änderungen anzupassen ist. Für die Verbraucher gilt insofern, als dies einen relativ großen Verwaltungsaufwand darstellen kann, vor allem, wenn man bedenkt, wie viele Dienste manche Personen nutzen. Von den Verbrauchern ist diesbezüglich eine gewisse Disziplin gefordert. Dies könnte jedoch dadurch erleichtert werden, dass bereits bei der Anmeldung bei einem Dienst auf die Möglichkeit und Vorteile der Vorsorge hingewiesen wird. Zudem kann es nie zwingend sein, eine vertragliche Vorsorge

[44] Insgesamt zum Folgenden vergleiche auch: *Gloser*, MittBayNot 2016, S. 101 (105).

zu treffen. Möchte ein Erblasser pauschal alle Online-Vertragsverhältnisse auf die Erben übertragen, kann dies daher auch durch Einsetzung eines Alleinerben erfolgen.

Insbesondere hinsichtlich des Erbfalls ist allerdings darauf hinzuweisen, dass solche vertraglichen Verfügungen strengen Anforderungen unterliegen und insbesondere nicht den gesetzlichen Regelungen zum Erbrecht widersprechen sowie die Testierfreiheit nicht unzulässig einschränken dürfen. Sind die Regelungen aber wirksam, können sie eine sinnvolle Alternative zur erbrechtlichen Übertragung darstellen. Diesbezüglich sollten die Dienstanbieter nicht nur ihre eigenen Interessen beachten, sondern auch die Interessen der Verbraucher an einer vertraglichen Regelung berücksichtigen.

Die vertraglichen Regelungen sind im Einzelfall an die Bedürfnisse der jeweiligen Vertragsbeziehung anzupassen. Ein Gedenkzustand ist nur sinnvoll, wenn Vertragsgegenstand ein Social-Media-Account oder sonst private Daten des Erblassers sind. Häufig wird die Inaktivität als der Umstand festgelegt, nach dem sich die Übertragung oder Löschung richtet. Dies hat zugegebenermaßen den Vorteil, dass keine sonstigen Nachweise für den Eintritt des Vorsorgefalls erbracht werden müssen. Kurzfristige Reaktionen auf Situationen, in denen ein schneller Zugriff notwendig wird, sind jedoch in diesem Fall kaum möglich. Auch kann die Inaktivität über einen gewissen Zeitraum auf einer freien Entscheidung beruhen, ohne dass eine Aktion hinsichtlich des Kontos gewünscht ist. Nach hier vertretener Ansicht sollte die Inaktivität daher nie alleiniger Umstand für die Ingangsetzung der Vorsorgeregelungen sein. Zusätzlich ist daher auch im Rahmen einer vertraglichen Regelung immer noch erforderlich, dass die Begünstigten dem Dienstanbieter den Sterbefall oder – zumindest in bestimmten Konstellationen – den Eintritt der Hilfsbedürftigkeit mitteilen.[45]

Eine Konfigurationsmöglichkeit des Dienstes wäre insbesondere auch dann sinnvoll, wenn neben dem ursprünglichen Nutzer gegebenenfalls zeitgleich ein Stellvertreter tätig werden soll.
Dies gilt zunächst dann, wenn der Stellvertreter nur ein beschränktes Recht auf Einsicht des Nutzerkontos haben soll. Hier könnte der Zugang des Stellvertreters so konfiguriert werden, dass nur die zur Einsichtnahme erforderlichen Funktionen freigeschaltet sind.
Eine gänzliche Sperrung der anderen Funktionen des Kontos des Nutzers ist dann nicht wünschenswert, da der Nutzer selbst möglicherweise diese Funktionen weiter gebrauchen will. Hat der Stellvertreter aber keinen eigenen Zugang, ist für den Dienstanbieter nicht erkennbar, ob sich bei einem konkreten Login-Vorgang der Nutzer selbst oder sein Stellvertreter anmeldet, sodass eine Differenzierung der Funktionen durch den Dienstanbieter nicht erfolgen kann. Es müsste insoweit darauf vertraut werden, als sich der Stellvertreter ordnungsgemäß verhält und nur die Funktionen verwendet, zu deren Nutzung er berechtigt ist. Eine Kontrolle des nur beschränkt ermächtigten Stellvertreters ist auf diese Weise kaum möglich. Meldet sich der Stellvertreter jedoch über einen eigenen Zugang auf dem Konto des Dienstanbieters an, ist für diesen erkennbar, dass der Stellvertreter handelt. Das Konto könnte in diesem Fall wieder so konfiguriert werden, dass nur die Funktionen freigeschaltet sind, zu deren Nutzung der Stellvertreter bevollmächtigt ist.

Ein weiterer Vorteil eines eigenen Zugangs des Stellvertreters würde auch darin bestehen, dass der Dienstanbieter den Nutzer gezielt über Anmeldevorgänge des Stellvertreters informieren könnte. So

[45] *Lange/Holtwiesche*, ErbR 2016, S. 487 (491).

könnte der Verbraucher durch den Dienstanbieter vor einem Missbrauch der Vollmacht zusätzlich geschützt werden. Hat der Stellvertreter keinen eigenen Zugang, müsste insoweit eine Warnung des Verbrauchers bei jeder neuen Anmeldung in seinem Nutzerkonto erfolgen. Daher würde der Verbraucher auch jedes mal benachrichtigt, wenn er sich selbst in seinem Konto einloggt.

Vor allem hinsichtlich der Stellvertreterkonstellation ergibt es daher Sinn, wenn eine Konfigurationsmöglichkeit in der Weise geschaffen würde, dass dem Stellvertreter – neben den Zugangsdaten des Nutzers – ein zweiter Satz Login-Daten zur Verfügung gestellt wird, über den er sich selbstständig im Konto des Nutzers anmelden kann.

7.3.3 Erweiterte Nutzung von Single Sign-On

7.3.3.1 Technische Darstellung und Bewertung

Die Nutzung und Problematik von Single Sign-On (SSO) zur Identitätsprüfung von Berechtigten wurden im Kapitel 6.8.6 auf Seite 273 betrachtet. Die mögliche Angabe von Vertrauenspersonen im Nutzerkonto wie es Google und Facebook ihren Nutzern in der Konfiguration des Nutzkontos ermöglichen, stellt eine Art SSO-Verfahren dar. Die Vertrauenspersonen haben allerdings im Sterbefall des Kontoinhabers nur begrenzte Zugriffsmöglichkeiten auf das Nutzerkonto, siehe Kapitel 7.3.2 auf Seite 305.

Dienstanbieter könnten die Übergabe des digitalen Nachlasses weiter erleichtern, indem sie in den vertraglichen Vereinbarungen mit den Nutzern auch die Login-Verfahren anderer Dienstanbieter für den Login von Begünstigten vorsehen. Dazu müsste es dem Kontoinhaber ermöglicht werden, in der Konfiguration seines Nutzerkontos die Begünstigten mit Namen und Kontodaten der anderen Dienste (z. B. den Facebook-Account eines Erben) zu hinterlegen. Über diese Erweiterung der Konfigurationsmöglichkeiten und Integration von SSO-Diensten erhalten die Dienstanbieter Kenntnis über Nutzerdaten anderer Dienste. Da der Nutzer die Kontaktdaten der Begünstigten selbst einträgt, braucht der Dienstanbieter die Zuordnung der SSO-Daten zu bestimmten Personen nicht unbedingt zu validieren. Der Dienstanbieter müsste die zulässigen SSO-Dienste in seine Webanwendung integrieren und im Erbfall den SSO-Login der Begünstigten für den Zugriff auf das Nutzerkonto des Erblassers freischalten.

Fazit: Die Integration von SSO-Diensten mit dem Ziel, Begünstigten des digitalen Nachlasses den Zugriff auf das Konto des Erblassers zu gewähren, erweitert die Vorsorgemöglichkeiten des digitalen Nachlasses. Dabei ist es wichtig, dass die Nutzer die Kontodaten ihrer Vertrauenspersonen selbst in ihrem Nutzerkonto hinterlegen können, weil dadurch eine relativ hohe Zuverlässigkeit der Daten erreicht werden kann, und der Dienstanbieter die SSO-Daten der Vertrauenspersonen nicht unbedingt validieren muss. Die SSO-Dienste der großen US-amerikanischen Anbieter sind allerdings hinsichtlich Datenschutz und Sicherheit fragwürdig, siehe Kapitel 7.3.2 auf Seite 305.

7.3.3.2 Rechtliche Bewertung

Die Nutzung eines Single Sign-On-Verfahrens bietet sich an, wenn ein Begünstigter zum ersten Mal gegenüber einem Dienstanbieter autorisiert werden soll. So kann verdeutlicht werden, dass sich nicht der Nutzer selbst, sondern ein Rechtsnachfolger oder Stellvertreter bei einem Konto anmeldet. Bieten die Dienstanbieter selbst ein solches Verfahren an, kann dies neben der Identifikation von Berechtigten auch dazu verwendet werden, um einen vertraglich vorgesehenen beschränkten Zugang (z. B. nur Einsichtsrecht mit Sperrung der Nachrichtenfunktion) zu gewähren.

Ein SSO-Login über ein Nutzerkonto eines anderen Dienstes ist auch in diesem Zusammenhang kritisch zu betrachten. Dies gilt jedenfalls hinsichtlich der SSO-Dienste der großen amerikanischen Anbieter. In diesem Fall ist einerseits zu beachten, dass nicht nur der Login ermöglicht wird, sondern in der Regel auch eine Verknüpfung des Nutzerkontos, bei dem die Anmeldung durchgeführt wird, mit dem Nutzerkonto des Dienstanbieters erfolgt. So kann der Dienstanbieter auf die Daten zugreifen, obwohl dies in diesem Zusammenhang nicht gewünscht ist. Dies ist auch unter Gesichtspunkten des Datenschutzrechts bedenklich. Andererseits können sich – wie im Rahmen der technischen Darstellung und Bewertung bereits beschrieben – Sicherheitsrisiken ergeben.

Denkbar ist insofern ein SSO-Login über den Dienst Verimi. Hier stellen sich nicht dieselben Bedenken wie gegenüber den amerikanischen Dienstanbietern.[46] Allerdings muss hierzu der Dienstanbieter, bei dem der Login erfolgen soll, mit dem Dienst Verimi kooperieren. Zudem muss der jeweilige Begünstigte über ein Nutzerkonto bei Verimi verfügen. Es ist jedoch nicht empfehlenswert, dass ein Verbraucher durch eine vertragliche Gestaltung gezwungen wird, sich bei einem solchen Dienst anzumelden, um von seiner Begünstigung oder Stellung als Stellvertreter Gebrauch zu machen. Eine derartige Anmeldung sollte auf der freien Entscheidung des Verbrauchers beruhen, insbesondere da auch im Rahmen von Verimi eine Datenspeicherung erfolgt.

7.3.4 Vertragsgemäße Hinterlegung von E-Mail-Adressen

7.3.4.1 Technische Darstellung und Bewertung

Eine Identitätsprüfung der Berechtigten durch deren Zugriff auf E-Mail-Konten, die der Erblasser zu Lebzeiten nicht in seinem Nutzerkonto hinterlegen konnte (oder wollte), wurde in Kapitel 6.8.2 auf Seite 264 betrachtet. Zur Unterstützung der Vorsorge durch den Nutzer wäre es hilfreich, wenn die Dienstanbieter den Nutzern zumindest ermöglichten, die Namen und E-Mail-Adressen von Vertrauenspersonen und Erben im Konto zu hinterlegen. Dann könnten sich im Sterbefall des Erblassers die Erben über den Zugriff auf ihre eigenen E-Mail-Konten gegenüber den Dienstanbietern identifizieren. Dienstanbieter könnten sich relativ gut darauf verlassen, dass es sich tatsächlich um die genannten Erben handelt. Denn die Namen und E-Mail-Konten wurden dem Dienstanbieter durch den betreffenden Erblasser selbst bekannt gemacht. Der Dienstanbieter könnte im Sterbefall des Erblassers eine E-Mail mit Link an die bekannten Adressen senden und von den Kontoinhabern erwarten, den Zugriff

[46] Siehe hierzu auch bereits in Kapitel 6.8.6.2 auf Seite 275.

durch Klick auf den Link zu bestätigen. Nach dieser Bestätigung könnte der Dienstanbieter den Erben dann die weiteren Schritte zur Ausübung ihrer Rechte ermöglichen.

Fazit: Geht es um die Wiedererkennung von bereits registrierten Kontoinhabern oder im Rahmen des digitalen Nachlasses um den Zugriff auf das Konto durch Vertrauenspersonen, deren Kontaktdaten vom Kontoinhaber hinterlegt worden waren, so kann der Nachweis, auf ein bestimmtes E-Mail-Postfach zugreifen zu können, für den Dienstanbieter ein zuverlässiger Hinweis sein, dass wirklich die genannte Person online anwesend ist. Eine Hinterlegung von Telefonnummern zusätzlich zu den E-Mail-Adressen ermöglicht eine noch zuverlässigere Überprüfung von Begünstigten, siehe Kapitel 7.3.5 auf der nächsten Seite.

7.3.4.2 Rechtliche Bewertung

Haben der Verbraucher und der Dienstanbieter vertraglich die Übertragung des Nutzerkontos oder die Zugriffsmöglichkeit eines Stellvertreters vereinbart, ist die Identifikation des Begünstigten durch ein E-Mail-Konto eine sinnvolle Alternative. Dies gilt dann, wenn die entsprechende E-Mail-Adresse bei dem Dienstanbieter im Rahmen der vertraglichen Vereinbarung hinterlegt wurde und die Nutzung des Kontos nach den gesetzlichen Voraussetzungen sonst von keiner speziellen Identitätsprüfung abhängig ist.[47] Macht der Begünstigte daher den Vorsorgefall geltend, könnte ihm zur Validierung ein zufälliger Bestätigungscode an die hinterlegte E-Mail-Adresse gesendet werden, mit der er sich gegenüber dem Dienstanbieter in dem von ihm festgelegten Verfahren legitimieren kann. Beispielsweise könnte das Verfahren vertraglich so ausgestaltet sein, dass sich der Begünstigte durch den Zugriff auf die E-Mail-Adresse gleichzeitig identifiziert und eigene Zugangsdaten erhält. Macht der Begünstigte beispielsweise geltend, dass der Erblasser gestorben ist, könnte der Dienstanbieter an die hinterlegte E-Mail-Adresse einen Bestätigungscode senden. Sind derjenige, der den Sterbefall geltend macht, und der Inhaber der E-Mail-Adresse identisch, kann auf diese Weise zunächst die Identifikation erfolgen. In einer weiteren E-Mail könnten dem Begünstigten dann neue Zugangsdaten zu dem Account des Verstorbenen übermittelt werden, durch die dieser die tatsächliche Zugriffsmöglichkeit auf das Nutzerkonto erhält. Um den Verbraucher vor einer missbräuchlichen Geltendmachung des Sterbefalls zu schützen, sind daran entweder gesonderte Anforderungen zu knüpfen (Vorlage einer Sterbeurkunde) und/oder der Nutzer ist vor der Herausgabe der Zugangsdaten an den vermeintlich Begünstigten zu informieren, damit er dem gegebenenfalls widersprechen kann.

Zwar ist denkbar, dass die hinterlegte E-Mail-Adresse im Vorsorgefall veraltet ist. Allerdings könnte der Verbraucher vertraglich verpflichtet werden, die Kontaktdaten aktuell zu halten. Auch ohne vertragliche Verpflichtung hat der Verbraucher aber grundsätzlich selbst ein Interesse daran, die Kontaktdaten zu aktualisieren, da auf diesem Wege dem vertraglich festgelegten Willen Geltung verschafft werden kann. Nur bei Aktualität der Kontaktdaten kann die Vertrauensperson wirksam die Mitteilungen vornehmen oder ein Begünstigter Zugriff erhalten.

[47] Im Rahmen der Identifikation gegenüber Online-Banken, die den allgemeinen Regeln für Banken unterliegen, ist die Identitätsprüfung über E-Mail daher nicht ausreichend. Diese müssten zusätzlich wohl ein Postident- oder Online-Ausweisprüfungs-Verfahren durchführen.

Hinsichtlich der Hinterlegung von E-Mail-Adressen ist auch zu beachten, dass sich der Dienstanbieter verpflichten sollte, die hinterlegte E-Mail-Adresse allein zu dem Zweck zu verwenden, um die vertragliche Vorsorgeregelung durchzusetzen. Eine weitere Nutzung zur Datenerhebung, zur Kundenbefragung oder zur Zusendung von E-Mails mit anderem Inhalt ist vertraglich zu untersagen.

7.3.5 Vertragsgemäße Hinterlegung von Telefonnummern

7.3.5.1 Technische Darstellung und Bewertung

Die Problematik der Identifikation von Personen über Telefonnummern wurde in Kapitel 6.8.5 auf Seite 271 beschrieben. Wenn Nutzer und Dienstanbieter die Übertragung eines Nutzerkontos vertraglich vereinbaren, kann die Hinterlegung der Namen und Telefonnummern von Begünstigten sinnvoll sein. Denn damit wären die Kontaktdaten dem Dienstanbieter frühzeitig und aus zuverlässiger Quelle bekannt und könnten im Sterbefall des Erblassers der Identifikation eines Begünstigten dienen. Der Dienstanbieter könnte beim Empfangen eines Anrufs oder einer E-Mail zur weiteren Absicherung auch den Zugriff auf das jeweils andere Konto überprüfen: Bei einem Anruf durch einen vorgeblich Begünstigten könnte der Dienstanbieter die Telefonnummer mit der hinterlegten Telefonnummer vergleichen und zusätzlich eine E-Mail mit Bestätigungslink an die betreffende Person senden, bevor das Nutzerkonto tatsächlich für den Begünstigten freigeschaltet wird. Umgekehrt könnte der Dienstanbieter beim Empfang einer E-Mail eines vorgeblich Begünstigten zunächst eine SMS mit Bestätigungscode an die entsprechende Telefonnummer senden. Die betreffende Person müsste dann den erhaltenen Bestätigungscode beispielsweise in ein Webformular eingeben, bevor der Dienstanbieter den Zugriff auf das Nutzerkonto des Erblassers freigibt.

Fazit: Wie in Kapitel 6.8.5 auf Seite 271 dargestellt, ist die Zuordnung von Telefonnummern zu Personen relativ fehleranfällig und bleibt über die Jahre nicht immer korrekt. Die Dienstanbieter könnten aber den Nutzern anbieten, Telefonnummern von Vertrauenspersonen, Bevollmächtigten und Erben in ihrem Nutzerkonto zu hinterlegen und im eigenen Interesse stets aktuell zu halten. Hinterlegte Kontaktdaten, bestehend aus Namen, Telefonnummern und E-Mail-Adressen, würden den Dienstanbietern relativ sichere und einfache Möglichkeiten bieten, mit den Begünstigten zu kommunizieren und ihnen die Ausübung ihrer Rechte zu ermöglichen.

7.3.5.2 Rechtliche Bewertung

Die Hinterlegung einer Telefonnummer eignet sich aus rechtlicher Sicht in ähnlicher Weise zur Identifikation eines Begünstigten wie eine E-Mail-Adresse, wenn Nutzer und Dienstanbieter die Übertragung eines Nutzerkontos vertraglich vereinbart haben. Insofern kann ein Bestätigungscode statt per E-Mail als SMS an den Begünstigten gesendet werden. Sind sowohl E-Mail-Adresse als auch Telefonnummer hinterlegt, könnte auch das im vorigen Kapitel 7.3.4.2 auf der vorherigen Seite beschriebene Verfahren weiter abgesichert werden. Zu beachten ist jedoch, dass möglicherweise eine begünstigte Person ihr Einverständnis verweigert, dass bei einem Dienstanbieter sowohl ihre E-Mail-Adresse

als auch ihre Telefonnummer hinterlegt werden, insbesondere wenn die Hinterlegung einer dieser Kontaktmöglichkeiten ausreichend sein kann.

Erklärt sich der Dienstanbieter vertraglich zu der Möglichkeit der Hinterlegung einer Telefonnummer bereit, so ist auch nicht zwingend erforderlich, dass die Identität über eine andere Stelle weiter überprüft wird. Der Verbraucher hinterlegt selbst die Telefonnummer des Begünstigten.[48] Da der Begünstigte im Vorsorgefall auf die eigenen Daten des Verbrauchers zugreifen kann, hat dieser zunächst selbst ein Interesse daran, nur die richtige Telefonnummer zu hinterlegen und diese auch aktuell zu halten. Zu letzterem könnte der Verbraucher auch vertraglich verpflichtet werden. Kümmert sich der Verbraucher nicht um die Aktualität der Kontaktdaten des Begünstigten, trägt er selbst das Risiko, dass seinem Willen nicht Rechnung getragen werden kann.

Auch die Telefonnummer sollte – wie soeben für E-Mail-Adressen beschrieben – allein zu dem Zweck der Durchführung der vertraglichen Vorsorgeregelung erfolgen. Eine weitergehende Nutzung wäre unzulässig.

7.3.6 Vergleich und Bewertung der genannten Verfahren

7.3.6.1 Aus technischer Sicht

Die Tabelle 7.1 vergleicht einige Eigenschaften technisch-organisatorischer Verfahren im Rahmen der vertraglichen Vorsorgemöglichkeiten in Anlehnung an die in Kapitel 6.8 auf Seite 262 genannten Kriterien. Hier bedeuten die in der Kopfzeile aufgeführten Kriterien Folgendes: „Qualität“ steht für die Korrektheit, Zuverlässigkeit und Sicherheit des Verfahrens. „Einfach (Nutzer)“ bedeutet, dass die Voraussetzungen für das Verfahren bei den meisten Nutzern bereits gegeben wären. Ein Verfahren gilt als „Kostenlos“, wenn aufseiten der Nutzer keine zusätzlichen Aufwände nötig werden, „Einfach (Anbieter)“ meint, dass der Dienstanbieter keinen hohen Aufwand hat, sich auf das Verfahren einzustellen. „Verbreitung“ schätzt, wie schnell sich das Verfahren auch international verbreiten könnte.

Verfahren	Qualität	Einfach (Nutzer)	Kostenlos	Einfach (Anbieter)	Verbreitung
Erweiterte Passw.-Fkt.	–	– –	o	–	o
Konfig. Dienste	++	+	++	o	++
Single Sign-On	o	+	+	+	+
E-Mail-Adressen	+	++	++	+	++
Telefonnummern	+	++	++	+	++

Tabelle 7.1: Technische Umsetzung vertraglicher Vorsorgemöglichkeiten

[48] Unter der Prämisse, dass sich der Begünstigte mit der Weitergabe seiner Kontaktdaten einverstanden erklärt hat.

Von den genannten Verfahren bietet nur die Konfiguration der Dienste umfassende Qualität und Sicherheit, weil der Dienstanbieter selbst das Interesse daran hat, dass systemeigene Funktionen auch gut funktionieren. Dafür muss allerdings der Anbieter zunächst ein grundsätzliches Interesse daran haben, die Möglichkeiten des digitalen Nachlasses für den Nutzer zu verbessern und den entsprechenden Integrationsaufwand zu leisten. Single Sign-On ist aus Sicht von Datenschutz und Sicherheit umstritten. E-Mail-Adressen und Telefonnummern können veralten, müssen also vom Nutzer in der Konfiguration stets aktuell gehalten werden.

Abgesehen von der erweiterten Passwort-Vergessen-Funktion mit Zusatzgeräten (und in der Regel zusätzlichen Passwörtern) sind die Verfahren aus Nutzersicht relativ einfach und preisgünstig, da die Voraussetzungen dafür meist bereits erfüllt sind. Die Verfahren könnten sich relativ schnell verbreiten bzw. sind bei vielen Diensten zumindest in Ansätzen bereits realisiert. So bieten viele Dienste bereits eine Zwei-Faktor-Authentisierung an, die zukünftig auch für eine erweiterte Passwort-Vergessen-Funktion und andere Verfahren genutzt werden könnte, um die Sicherheit zu erhöhen. Single Sign-On wird bereits in großem Ausmaß verwendet, wenn auch nicht im Rahmen des digitalen Nachlasses. Mit dem Speichern von E-Mail-Adressen und Telefonnummern sind die meisten Nutzer und Dienstanbieter vertraut. Allerdings können bei einer zunehmenden Speicherung von Kontaktdaten (über die Daten des Kontoinhabers hinaus) Datenschutzfragen verstärkt in den Vordergrund rücken.

Die folgende Tabelle 7.2 gibt einen Überblick über die Vor- und Nachteile der technisch-organisatorischen Verfahren im Rahmen der vertraglichen Vorsorgemöglichkeiten.

Tabelle 7.2:
Technisch-organisatorische Verfahren im Rahmen der vertraglichen Vorsorgemöglichkeiten mit ihren Vor- und Nachteilen

Lösung	Vorteile	Nachteile
Erweiterung Passwort-Vergessen-Funktion	✓ Neusetzen einer E-Mail-Adresse möglich ✓ Begünstigte müssen keinen Zugriff auf das E-Mail-Konto des Erblassers haben	✗ Erfordert aufwendigere Sicherheitsvorkehrungen (z. B. 2-Faktor-Authentisierung)
	✓ Inaktivitätsmanager mit DeathSwitch möglich	✗ Inaktivität sollte nie allein die Vorsorgeregelungen anstoßen
	✓ Separater Zugang für Stellvertreter möglich	✗ Zugriffsrechte müssten vorab definiert werden
Erweiterte Konfigurationsmöglichkeiten der Dienste	✓ Ermöglicht selbstbestimmte, klar definierte Vorsorge	✗ Hoher Konfigurationsaufwand für Nutzer bei vielen Konten ✗ Lösungen von Interessen der Anbietern bestimmt ✗ Nutzungsbedingungen können sich ändern

Fortsetzung auf der nächsten Seite

Tabelle 7.2: Technisch-organisatorische Verfahren im Rahmen der vertraglichen Vorsorgemöglichkeiten mit ihren Vor- und Nachteilen (Fortsetzung)

Lösung	Vorteile	Nachteile
	✓ Verfügungen und Nachweise nicht unbedingt erforderlich	✗ Vertragliche Verfügungen widersprechen evtl. dem Erbrecht
Erweiterte Nutzung von Single Sign-On	✓ Zuverlässig, da Kontoinhaber selbst die Daten der Begünstigten hinterlegt ✓ Login der Begünstigten ermöglicht es, deren Zugang zu beschränken	✗ Datenschutz sozialer Netzwerke fragwürdig
	✓ SSO-Plattform Verimi ist deutsch-europäisch	✗ Begünstigte müssen Verimi-Konto haben ✗ Anbieter müssen Partner von Verimi werden
Vertragliche Hinterlegung von E-Mail-Adressen	✓ Voraussetzungen gegeben und unkompliziert ✓ Zuverlässig, da Kontoinhaber selbst die Daten der Begünstigten hinterlegt ✓ Gut kombinierbar mit zusätzlicher Hinterlegung der Telefonnummern	✗ Begünstigte müssen in die Verarbeitung der Daten einwilligen ✗ Kontoinhaber muss die Daten aktuell halten ✗ Anbieter könnten die Daten auch für andere Zwecke verwenden
Vertragliche Hinterlegung von Telefon-nummern	✓ Voraussetzungen gegeben und unkompliziert ✓ Zuverlässig, da Kontoinhaber selbst die Daten der Begünstigten hinterlegt ✓ Gut kombinierbar mit zusätzlicher Hinterlegung der E-Mail-Adressen	✗ Begünstigte müssen in die Verarbeitung der Daten einwilligen ✗ Kontoinhaber muss die Daten aktuell halten ✗ Anbieter könnten die Daten auch für andere Zwecke verwenden

7.3.6.2 Aus rechtlicher Sicht

Aus rechtlicher Sicht würde sich eine Kombination der verschiedenen Möglichkeiten anbieten. Insgesamt ist für eine umfassende vertragliche Regelung wie in Kapitel 7.2 auf Seite 292 beschrieben eine Konfiguration der Dienste erforderlich. Nach der hier vertretenen Auffassung ist es sinnvoll, wenn der Dienstanbieter verschiedene Auswahlmöglichkeiten zur Verfügung stellt, was im Vorsorgefall mit dem Nutzerkonto geschehen soll. Insofern können die vertraglichen Gestaltungsmöglichkeiten für den Fall der Handlungsunfähigkeit und des Todesfalls auch nebeneinander angeboten werden, um eine umfassende Regelung der Fälle, die eine Vorsorge erfordern, zu ermöglichen. Die Dienste wären somit so zu konfigurieren, dass im vertraglich festgelegten Zeitpunkt eine Löschung, eine beschränkte oder vollständige Übertragung auf einen Begünstigten oder gar keine Regelung möglich ist. Für Social-Media-Konten könnte zusätzlich ein Gedenkzustand vorgesehen werden.

Um vom Vorsorgefall zu erfahren, können E-Mail-Adressen oder Telefonnummern von Vertrauenspersonen hinterlegt werden, die dem Dienstanbieter den Eintritt des Vorsorgefalls mitteilen bzw. die im Vorsorgefall Zugriff auf Nutzerkonten erhalten sollen. Hinsichtlich des Zugriffs von Begünstigten wäre grundsätzlich auch ein Single Sign-On-Verfahren möglich, allerdings wird aufgrund der bereits beschriebenen Nachteile eher die Hinterlegung von E-Mail-Adressen oder Telefonnummern empfohlen. Zum Schutz des Verbrauchers müsste der Dienstanbieter aber verpflichtet werden, die hinterlegten Kontaktdaten allein zur Abwicklung des festgelegten Vorsorgefalls zu verwenden und den Verbraucher nicht aus anderen Gründen zu kontaktieren.

Insbesondere im Fall der Stellvertretung wäre es zudem – wie in Kapitel 7.3.1.2 auf Seite 304 beschrieben – sinnvoll, wenn der Stellvertreter sich über eigene Zugangsdaten bei dem Nutzerkonto des Verbrauchers anmelden müsste. Dies gilt vor allem dann, wenn der Stellvertreter nicht zu einer umfassenden Verwaltung eines Nutzerkontos berechtigt sein, sondern lediglich ein Einsichtsrecht erhalten soll.

7.4 Nachweismöglichkeiten über den Tod des Erblassers

Ist vertraglich das Versterben des Nutzers als Vorsorgefall vorgesehen, muss der Dienstanbieter vom Eintritt dieses Ereignisses zuverlässig erfahren können.

Aus rechtlicher Sicht wird der Tod des Erblassers in der Regel durch Vorlage einer Sterbeurkunde (§§ 55 I Nr. 5, 60 PStG) nachgewiesen. Möglich ist auch der Nachweis durch eine beglaubigte Abschrift aus dem Sterberegister (§§ 55 I Nr. 1, 31 I Nr. 4 PStG). Zuständig hierfür ist das Standesamt. Wenn die Sterbeurkunde noch nicht in einem zentralen Register i. S. d. § 67 PStG erfasst ist, ist für die Ausstellung der Urkunde das registerführende Standesamt zuständig, außer einem anderen Standesamt können die erforderlichen Daten elektronisch übermittelt werden, § 55 II PStG. Ist die Urkunde aber in einem zentralen Register erfasst, kann die Urkunde von jedem Standesamt erstellt werden, das Zugriff auf das Register hat, § 67 III PStG. Die Urkunde wird in Papierform ausgestellt.

Der Sterbefall kann aber in der Regel auch durch Vorlage des eröffneten Testaments in Verbindung mit dem Eröffnungsbeschluss nachgewiesen werden. Dies ist einerseits dann möglich, wenn sich das Testament in amtlicher Verwahrung befindet. In amtlicher Verwahrung befindet sich ein Testament entweder, wenn es sich um ein öffentliches Testament i. S. d. § 2232 BGB handelt, da der Notar verpflichtet ist, das Testament unverzüglich in besondere amtliche Verwahrung zu bringen, § 34 I 4 BeurkG. Daneben ist auch ein eigenhändiges Testament nach § 2248 BGB auf Verlangen des Erblassers vor seinem Tod in besondere amtliche Verwahrung zu nehmen. Ist dies nicht geschehen, besteht daneben eine Ablieferungspflicht des unmittelbaren Besitzers[49] nach § 2259 I BGB oder der Behörde, die nicht das Eröffnungsgericht ist,[50] nach § 2259 II BGB. Da das Testamentseröffnungsverfahren nur durchgeführt wird, wenn das Gericht vom Tod des Erblassers Kenntnis erlangt (§ 348 I 1 FamFG), ist durch den Eröffnungsbeschluss inzident der Tod des Erblassers bewiesen. Gleiches

[49] *Sticherling*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2259 Rn. 14 f.
[50] *Sticherling*, in: Säcker u. a. (Hrsg.), MükoBGB, § 2259 Rn. 18 f.

gilt, wenn bei fehlender letztwilliger Verfügung ein Erbschein für den gesetzlichen Erben ausgestellt wurde. Auch im Verfahren auf Erteilung eines Erbscheins wird gemäß § 352 I Nr. 1, III FamFG der Erbschein nur erteilt, wenn durch öffentliche Urkunden der Todeszeitpunkt des Erblassers bewiesen ist. Insoweit können die Erben sowohl den Tod des Nutzers als auch ihre Erbberechtigung in einem Schritt nachweisen.[51]

Grundsätzlich gilt, dass allein durch die Vorlage einer Sterbeurkunde nur bewiesen ist, dass der Nutzer verstorben ist. Den Erben hilft das insofern nicht weiter, als damit noch nicht ihre Berechtigung als Erben nachgewiesen ist und die Dienstanbieter ihnen allein durch den Nachweis des Todes noch keinen Zugang zu dem Account gewähren müssen. Hierzu ist dem Dienstanbieter immer auch ein Erbschein oder eine eröffnete letztwillige Verfügung vorzulegen, woraus die Erbenstellung eindeutig hervorgeht. Durch die Vorlage eines Erbscheins oder einer eröffneten letztwilligen Verfügung ist jedoch – wie soeben beschrieben – zugleich der Sterbefall bewiesen, sodass die Vorlage der Sterbeurkunde obsolet ist.

Die Vorlage der Sterbeurkunde allein kann allerdings dann Sinn ergeben, wenn die Rechtsnachfolger nicht durch Erbrecht, sondern durch vertragliche Regelung mit dem Dienstanbieter bestimmt wurden. In diesem Fall ist der Rechtsnachfolger nicht durch Erbrecht, sondern durch die vertragliche Regelung begünstigt. Somit müssen keine Erbnachweise vorgelegt werden, sondern lediglich der Todesfall – als das vertraglich bestimmte Ereignis für die Rechtsnachfolge – bewiesen werden.

7.4.1 Bestätigung durch Vertrauenspersonen

Um die Dienstanbieter in die Übergabe des digitalen Nachlasses einzubeziehen, muss es Maßnahmen geben, wie die Dienstanbieter die Information über einen Sterbefall aus einer zuverlässigen Quelle erhalten. Aus Sicht vieler Online-Dienste wie Passwort-Manager oder Dokumentarchive reicht dazu ein sogenannter DeathSwitch (siehe Kapitel 6.5.4.1 auf Seite 200 und die folgenden Kapitel 7.4.1.1 auf der nächsten Seite und 7.4.1.2 auf Seite 319), um auf Wunsch des Kontoinhabers die Login-Daten und den Zugriff auf ausgewählte Informationen an andere Personen durchzuführen. Bisher sind nur wenige international agierende Dienstanbieter wie PayPal bereit, amtliche Sterbeurkunden zu prüfen. Denn dies ist ein sehr aufwendiger Prozess, solange die Urkunden nicht in standardisierter digitaler Form vorliegen, sondern in Papierform mit Inhalten in Format und Amtssprache des jeweiligen Landes, siehe Kapitel 7.4.2.1 auf Seite 322 und 7.4.2.2 auf Seite 323.

Im Folgenden werden mögliche Alternativen vorgestellt, wie der Sterbefall des Erblassers dem Dienstanbieter mitgeteilt werden kann. Wichtige Kriterien hierfür sind:

- **Sicherheit**: Ist die Mitteilung des Sterbefalls zuverlässig und verbindlich? Kann der Dienstanbieter nachvollziehen, von wem die Information kommt?

[51] A. A. wohl *Brisch/Müller-ter Jung*, CR 2013, S. 446 (451), die anscheinend stets auch die Vorlage der Sterbeurkunde für notwendig erachten.

- **Datenschutz**: Ist ein versehentliches Auslösen der Mitteilung und das versehentliche Freigeben von Dokumenten ausgeschlossen?
- **Gebrauchstauglichkeit**: Ist es für die Angehörigen leicht, den Dienstanbietern den Sterbefall mitzuteilen? Ist der Nachweis des Sterbefalls leicht zu erzeugen oder zu beschaffen?

7.4.1.1 Einfache Bestätigung einer Inaktivitätsfeststellung

Eine einfache Bestätigung des Sterbefalls an den Dienstanbieter durch Vertrauenspersonen wird beispielsweise auf folgende Weise mithilfe eines DeathSwitch ermöglicht: Der Kontoinhaber hinterlegt zu Lebzeiten die Kontaktdaten der Vertrauenspersonen in den Einstellungen des Dienstes. Zusätzlich konfiguriert er die Frist, in der er gegenüber dem Dienst inaktiv sein darf, ohne als verstorben zu gelten (z. B. 1, 3 oder 6 Monate). In der Nutzungsphase kontrolliert der Dienst, wie viel Zeit seit seinem letzten Login (oder einer anderen Nutzeraktivität) verstrichen ist. Ist die Frist ohne Nutzeraktivität verstrichen, sendet der Dienst automatisch eine Nachricht an den Kontoinhaber mit der Aufforderung, sich in das Nutzkonto einzuloggen oder zumindest auf die Nachricht zu antworten. Kommt der Nutzer diese Aufforderung innerhalb einer weiteren Frist nicht nach, sendet der Dienst eine Nachricht an die Vertrauenspersonen mit der Bitte, den vermuteten Sterbefall entweder zu bestätigen oder zu entkräften.

Der Identitätsnachweis der benachrichtigten Vertrauenspersonen besteht dabei in der Regel im nachgewiesenen Zugriff auf hinterlegte E-Mail-Konten oder Telefonnummern, vgl. die Kapitel 7.3.4 auf Seite 310 und 7.3.5 auf Seite 312. Die Dienstanbieter nehmen dabei an, dass Kontoinhaber ein großes Interesse daran haben, die Kontaktdaten vertrauenswürdiger Personen korrekt zu hinterlegen. Die Vertrauenspersonen müssen gegenüber den Dienstanbietern nicht nachweisen, wer sie sind. Die durch den DeathSwitch weitergegebenen Inhalte (z. B. Passwörter) stellen nicht unbedingt schon die digitalen Werte an sich da, können aber den Zugriff auf digitale oder auch physische Werte ermöglichen.

DeathSwitches stützen sich meist darauf, dass der Kontoinhaber über ein ablaufendes Zeitintervall nicht auf bestimmte E-Mails oder SMS des Dienstes reagiert, wodurch der Prozess wieder auf das volle Zeitintervall zurückgesetzt werden würde. Diese Art der Feststellung kann fehleranfällig sein, da es viele Gründe geben kann, warum E-Mails oder SMS für gewisse Zeit unbeantwortet bleiben. Eine fortgeschrittene DeathSwitch-Anwendung könnte das Smartphone des Kontoinhabers über die Nutzung von SMS hinaus stärker berücksichtigen, da die meisten Nutzer ihr Smartphone fortwährend mit sich führen und viele Male am Tag nutzen. Die Anwendung könnte die Aktivität des Smartphones selbst oder auch dessen wechselnde Lokalisierung als Lebenszeichen des Nutzers werten. Umgekehrt wäre aber ein längerer Stillstand des Smartphones kein hinreichender Grund dafür, gleich einen Notfall oder Todesfall anzunehmen. Der Inhaber könnte stattdessen auch im Urlaub oder Retreat sein und sein Handy einfach für längere Zeit abgeschaltet haben. Auch wenn das Smartphone defekt ist oder sich die Akkuladung trotz Nichtbenutzung nach wenigen Tagen erschöpft, würde der Dienst keine Aktivitätsmeldung mehr empfangen.

Sowohl Kontoinhaber als auch Dienstanbieter haben ein großes Interesse daran, einen Notfallverdacht zunächst durch ein oder mehrere Vertrauenspersonen bestätigen zu lassen, bevor ein DeathSwitch ausgelöst und Zugangsinformationen verteilt werden. Eine zuvor festgelegte Zahl von Vertrauenspersonen sollte übereinstimmend antworten, sodass der Dienst auf dieser Grundlage eine Entscheidung treffen kann. Die Vertrauenspersonen klicken dazu beispielsweise auf einen Link in der E-Mail, gelangen auf eine Webseite des Dienstes und geben dort ein, ob tatsächlich ein Notfall eingetreten ist. Dieses Eingabeformular könnte durch ein individuelles Passwort geschützt sein, das der Dienst zuvor jeder Vertrauensperson per SMS zugesendet hat.

DeathSwitch-Lösungen der Dienstanbieter sind zwar dienstspezifisch, können aber aus Sicht der Nutzer eine selbstbestimmte Vorsorge ermöglichen. Beispielsweise können Nutzer mit Googles Kontoinaktivität-Manager bestimmte Kontodaten mit anderen Nutzern teilen oder andere Nutzer im Notfall oder Sterbefall automatisch benachrichtigen.[52] Die Nutzer können selbst konfigurieren, wie lange die Konteninaktivität dauern darf und welche Personen Zugriff auf die Google-Konten erhalten sollen. Das ermöglicht eine einfache Abwicklung gemäß den Willensbekundungen der Kontoinhaber, ohne dass der Dienstanbieter Sterbeurkunden oder Erbscheine prüfen müsste. Kontrollnachrichten gehen zunächst an den Kontoinhaber, dann an die eingetragenen Kontaktpersonen. Schließlich bekommen die Kontaktperson(en) eine E-Mail mit der Auflistung der freigegebenen Daten und einen Link zum Herunterladen dieser Daten. An die Mobiltelefonnummern der Kontaktpersonen wird per SMS ein Bestätigungscode gesendet, der als eine Art Identitätsnachweis für den Zugriff dient.

Fazit: DeathSwitches sollten so konfigurierbar sein, dass mehrere Vertrauenspersonen einbezogen werden, die gegenüber dem Dienstanbieter den Sterbefall des Erblassers bestätigen müssen. Ein bloßes Ausbleiben der Online-Aktivitäten des Erblassers darf für Dienstanbieter kein hinreichender Grund sein, den Sterbefall anzunehmen und den Zugriff auf persönliche Daten des Kontoinhabers für andere Personen freizuschalten. In jedem Fall sollten Dienstanbieter zumindest weitere Prüfungen vornehmen, beispielsweise die automatische Suche nach Aktivitäten des Kontoinhabers in sozialen Netzwerken, wenn der Kontoinhaber das Nutzerkonto mit weiteren Konten (z. B. Twitter, Instagram) verknüpft hat. Solche zusätzlichen Prüfungen könnten den Dienstanbietern in Form einer Nachweispflicht von Sterbefällen auferlegt werden. An weitergehenden Konfigurationslösungen der Dienstanbieter wie dem Google Kontoinaktivität-Manager wird von rechtlicher Seite kritisiert, dass die Dienstanbieter mit solchen Konfigurationsmöglichkeiten quasi-testamentarische Lösungen schaffen, die existierende erbrechtlichen Vorschriften einfach umgehen oder ihnen widersprechen.[53,54]

7.4.1.2 Kryptografisch unterstützte Bestätigung einer Inaktivitätsfeststellung

Möchte der Dienst verhindern, dass die Vertrauensperson den Link und das Passwort beabsichtigt oder unbeabsichtigt an andere Personen weitergibt, so könnte das Bestätigungsverfahren im Hintergrund kryptografisch an das Gerät gebunden werden, mit dem eine Vertrauensperson die Be-

[52] Google Kontoinaktivität-Manager, https://support.google.com/accounts/answer/3036546?hl=de.

[53] *Funk*, Das Erbe im Netz: Rechtslage und Praxis des digitalen Nachlasses, S. 36.

[54] *Schmid u. a.*, Sterben im Internet – Regelung des digitalen Nachlasses, in: Wirtschaftsinformatik & Management 5.1, S. 87 und S. 94.

nachrichtigung bearbeitet, ohne dass Passwörter eingegeben werden müssen. Dazu wird mit dem Benachrichtigungslink ein kryptografischer Schlüssel heruntergeladen und in eine dienstspezifische Anwendung integriert. Die notwendige Bestätigung durch mehrere Personen lässt sich beispielsweise mit einem kryptografischen Schwellenwert-Signaturverfahren („k-out-of-n Threshold Signature“) realisieren.[55] Dazu müssen mindestens k von n Mitgliedern der zuvor festgelegten Gruppe (beispielsweise von Vertrauenspersonen) zusammenarbeiten, um eine Nachricht zu signieren. Die Verfahren haben herkömmliche Signaturverfahren wie RSA, DSA oder ECDSA auf eine Weise modifiziert, dass ein Signaturschlüssel in Form von mehreren Teilschlüsseln an die Teilnehmer verteilt wird. Die Anwendung einer gewissen Zahl von Teilschlüsseln reicht dabei aus, um eine gültige Signatur zu erstellen. Ein solches Verfahren hat die Eigenschaft, dass die Identität der beteiligten Teilnehmer gegenüber einem Dritten, der nur an der Echtheit der signierten Nachricht interessiert ist, geheim bleiben kann. Zudem kann der Signaturschlüssel relativ leicht geheim gehalten werden, dadurch, dass er auf keinem Gerät als vollständiger Schlüssel vorliegen muss. Und so könnte ein solches Verfahren praktisch angewendet werden:

Schritt 1: Der Kontoinhaber konfiguriert zu Lebzeiten den DeathSwitch, indem er die Kontaktdaten von mehreren Vertrauenspersonen beim Online-Dienst hinterlegt.

Schritt 2: Der Online-Dienst generiert serverseitig ein Schlüsselpaar (privater Signaturschlüssel und öffentlicher Signaturprüfschlüssel), trennt den privaten Signaturschlüssel in mehrere Teilschlüssel auf und legt jeweils einen Teilschlüssel zu den Daten einer jeden Vertrauensperson.

Schritt 3: Zur Überprüfung eines Sterbefallverdachts werden die Vertrauenspersonen aufgefordert, ihre Teilschlüssel herunterzuladen und innerhalb eines bestimmten Zeitintervalls entweder die Nachricht „Kontoinhaber ist gestorben“ oder die Nachricht „Kontoinhaber lebt noch“ mit ihrem Teilschlüssel zu signieren.

Schritt 4: Der Dienst empfängt die signierten Antworten. Wenn die zuvor festgelegte Mindestzahl von Vertrauenspersonen geantwortet hat, fügt der Dienst die Antworten zusammen und verifiziert deren Echtheit mit dem Signaturprüfschlüssel.

Schritt 5: Der Sterbefallverdacht gilt mit einer zuvor festgelegten Mindestzahl von Antworten „Kontoinhaber ist gestorben“ als bestätigt, sodass der Dienst schließlich das mit dem Kontoinhaber vereinbarte Nachlassverfahren einleitet.

Fazit: Kryptografische DeathSwitches könnten im Vergleich zu einfachen DeathSwitches mehr Sicherheit und Datenschutz bieten, indem die Bestätigungen des Sterbefalls durch die Vertrauenspersonen beim Dienstanbieter kryptografisch gebündelt und abgesichert werden, sodass eine versehentliche Freigabe der Daten unwahrscheinlicher ist. Der Aufwand ist aber auf beiden Seiten sehr hoch, denn die Nutzer müssen für die Lösung spezielle Programme installieren, die wahrscheinlich nicht geräteübergreifend einsetzbar sind. Die Anbieter haben den Aufwand, ein angemessenes kryptografisches Konzept zu erarbeiten und zu implementieren. Sie müssen beispielsweise pro Anwendungsfall die geeigneten kryptografischen Parameter bestimmen können.

[55] *Brandão/Mouha/Vassilev*, NISTIR 8214.

7.4.1.3 Rechtliche Bewertung

Ist vertraglich zwischen dem Nutzer und dem jeweiligen Dienstanbieter im Einzelfall vereinbart, dass eine dritte Person im Vorsorgefall Zugriff auf das Nutzerkonto erhalten soll, ist jedenfalls im Sterbefall der Tod des Nutzers und damit der Eintritt des vertraglich vereinbarten Zeitpunkts des Übergangs der Vertragsbeziehung zu beweisen. Auch wenn die vertragliche Vereinbarung vorsieht, dass nach dem Tod des Nutzers das Nutzerkonto gelöscht werden soll, ist der Sterbefall zu beweisen. In dem Fall, dass vertraglich keine Vereinbarung zwischen Nutzer und Dienstanbieter über den Übergang des Vertragsverhältnisses stattgefunden hat, kann der Nachweis des Todesfalls allein nie ausreichen. Vielmehr ist die Erbenstellung des Rechtsnachfolgers gegenüber dem Dienstanbieter durch Vorlage eines Erbscheins oder einer eröffneten letztwilligen Verfügung zu beweisen. Der isolierte Beweis des Todesfalls, beispielsweise durch Vorlage der Sterbeurkunde, ist in diesem Fall – wie oben bereits beschrieben – obsolet.

Da die Nutzung von kommerziellen Diensten, die eine DeathSwitch-Funktion anbieten, eher kritisch zu sehen ist,[56] müsste der Dienstanbieter des jeweiligen Portals, gegenüber dem der Todesfall bestätigt werden soll (z. B. Facebook, Twitter, PayPal etc.), selbst einen DeathSwitch anbieten.

Wie ebenfalls oben bereits beschrieben, ist Nachteil des erforderlichen Ablaufs eines Zeitintervalls zur Auslösung des DeathSwitch, dass es nicht möglich ist, auf dringende Fälle zu reagieren. Demgegenüber hat eine reine Bestätigung des Sterbefalls durch eine Vertrauensperson den Vorteil, dass diese zeitnah nach dem Todesfall erfolgen kann. Zwar ist diese Bestätigung des Sterbefalls durch Vertrauenspersonen kein rechtlich verbindlicher Beweis des Ereignisses. Ist eine solche Bestätigung aber vertraglich zwischen dem Nutzer und dem jeweiligen Dienstanbieter vereinbart – wenn sich letztlich der Dienstanbieter mit der Bestätigung als Beweis begnügt – könnte dies grundsätzlich die Vorlage einer Sterbeurkunde ersetzen.

Zu bedenken ist jedoch, dass einerseits die Benennung mehrerer Vertrauenspersonen gegenüber jedem Dienstanbieter für den Verbraucher relativ aufwendig ist. Auch wenn der Nutzer gegenüber jedem Dienstanbieter dieselben Vertrauenspersonen benennen kann, ist der Nutzer doch dafür verantwortlich, deren Kontaktdaten – möglicherweise über mehrere Jahrzehnte – aktuell zu halten. Daneben ist die Verwendung eines kryptografischen Schlüssels ein für Dienstanbieter und Vertrauensperson sehr aufwendiges Verfahren. Andererseits müssen die Vertrauenspersonen zuverlässig sein. Dabei besteht zunächst die Gefahr, dass die Vertrauensperson ihre Stellung missbraucht. Zwar ist diese Gefahr reduziert, wenn mehrere Vertrauenspersonen gemeinsam die Bestätigung durchführen müssen. Allerdings kann die Gefahr auch dadurch nicht gänzlich ausgeschlossen werden.

Zudem können Vertrauenspersonen auch in dem Sinne unzuverlässig sein, als sie ihr zur Bestätigung notwendiges Passwort vergessen oder das für den kryptografischen Schlüssel notwendige Programm nicht pflegen. Auch hier ist wieder zu bedenken, dass zwischen Vorsorge und Sterbefall mehrere Jahrzehnte vergehen können. Über diesen Zeitraum ist auch nicht unwahrscheinlich, dass Nutzer und Vertrauensperson den Kontakt abbrechen und die Vertrauensperson schlicht kein Interesse mehr hat, die Bestätigung gegenüber dem Anbieter durchzuführen. Allerdings ist der Verbraucher selbst dafür

[56] Siehe dazu bereits ausführlich oben.

verantwortlich, gegenüber dem Dienstanbieter eine Person zu benennen, die nicht bereits aus diesen persönlichen Gründen die Bestätigung verweigert. Der Dienstanbieter müsste hierfür die Möglichkeit eröffnen, die Einstellungen hinsichtlich der Vertrauensperson zu ändern und eine neue Person zu benennen.

Die Bestätigung durch eine oder mehrere Vertrauenspersonen ist somit im Rahmen einer vertraglichen Regelung grundsätzlich möglich, auch wenn das Risiko der Unzuverlässigkeit besteht. Diese Bestätigung kann, muss aber nicht mit dem Ablauf eines Zeitintervalls verbunden werden. So ist eine vertragliche Regelung dahingehend denkbar, dass die Vertrauensperson im Sterbefall auf den Dienstanbieter zukommt. Um hier das Missbrauchsrisiko durch die Vertrauensperson zu senken, sollte die Erklärung der Vertrauensperson durch einen weiteren Nachweis des Sterbefalls begleitet werden.

7.4.2 Sterbeurkunden

7.4.2.1 Herkömmliche Sterbeurkunden

Einige Dienste, mit denen hohe finanzielle Transaktionen durchgeführt werden können, wie Onlinebanking oder Online-Bezahldienste, verlangen für die Übergabe eines digitalen Nachlasses den direkten Nachweis einer amtlichen Sterbeurkunde. Eine Sterbeurkunde wird in Deutschland aufgrund eines vorhandenen Totenscheins ausgestellt.[57] Auf Grundlage des Totenscheins erstellt das zuständige Standesamt gemäß § 31 PStG einen Eintrag in das elektronische Sterberegister und stellt eine Sterbeurkunde aus.[58] Jeder Eintrag im Sterberegister wird von einem Standesbeamten mit einer qualifizierten elektronischen Signatur versehen. Die Bundesländer können gemäß § 67 PStG zentrale Sterberegister einrichten, auf die alle angeschlossenen Standesämter Zugriff haben. Auskunftsberechtigt für Informationen aus dem Personenstandsregister sind nach § 62 PStG die Betroffenen selbst und ihre Familienangehörigen, außerdem solche Personen, die ein rechtliches Interesse glaubhaft machen können.

Behörden verschiedener europäischer Länder können internationale Sterbeurkunden im Sterberegister der Internationalen Kommission für das Zivil- und Personenstandswesen (Commission Internationale de l'Etat Civil, CIEC) abrufen.[59] Elektronische Sterbeurkunden sind aber bisher nicht möglich,

[57] Der Totenschein ist eine öffentliche, von einem Arzt ausgestellte Urkunde, die den Tod eines Menschen bescheinigt. Sie besteht aus vier Papierblättern, die auf zwei Briefumschläge verteilt werden, einen vertraulichen und einen nicht-vertraulichen Teil. Der nicht-vertrauliche Teil enthält u. a. die Personenangaben Vor- und Nachname, Geschlecht, Wohnadresse, Geburtstag und Geburtsort, Sterbezeitpunkt und Sterbeort.

[58] Ein Sterberegistereintrag beinhaltet folgende Daten des Verstorbenen: Vorname(n), Nachname, Geburtsort, Geburtstag, Geschlecht, Zeitpunkt und Ort des Todes, letzter Wohnsitz, Familienstand, Verweise auf Geburts- und ggf. Heiratsurkunde, auf Wunsch des Anzeigenden die rechtliche Zugehörigkeit des Verstorbenen zu einer rechtlich anerkannten Religionsgemeinschaft; ggf. Vorname(n), Nachname und Geschlecht des (letzten) Ehegatten oder Lebenspartners. Gemäß § 21 PStG wird jedes Kind über dessen Geburtseintrag mit den Geburtseinträge seiner Eltern verlinkt.

[59] Die CIEC ist eine zwischenstaatliche Organisation mit dem Ziel, die internationale Zusammenarbeit auf den Gebieten des Personenstandsrechts, Familienrechts und Staatsangehörigkeitsrechts zu verbessern. Die 15 CIEC-Mitgliedsstaaten sind: Belgien, Frankreich, Griechenland, Großbritannien, Italien, Kroatien, Luxemburg, Niederlande, Österreich, Polen,

da einige Länder wie die Schweiz weiterhin Urkunden nur auf speziellem Sicherheitspapier ausgeben möchten. Außerdem besteht beispielsweise in der Schweiz keine Rechtsgrundlage dafür, dass privatwirtschaftliche Dienste direkt auf das CIEC-Todesregister zugreifen dürfen.[60] Auf europäischer Ebene ist mit der VO (EU) 2016/1191 vom 6. Juli 2016 festgelegt, dass die EU-Mitgliedsstaaten gegenseitig die Urkunden ihrer Bürger anerkennen, und eine Übersetzung von Urkunden in die Amtssprache eines anderen Mitgliedsstaates mittels Ausgabe mehrsprachiger Formulare vereinfacht wird.[61] Damit lassen sich Sterbefälle in der gesamten Europäischen Union gut nachweisen. Zudem wird seit Anfang 2018 an der Harmonisierung von Personenstandsurkunden (Geburts-, Heirats- und Sterbeurkunden) in Hardware-, Papier- und Server-basierten Prozessen gearbeitet.[62] Erwartet wird, dass für alle drei Urkundentypen in etwa die gleichen Prozesse anwendbar sein werden. Voraussichtlich wird es dennoch viele Jahre dauern, bis ein vollständiger Standard vorliegt. Die Standardisierungsbemühungen haben den Anspruch, dass Bürger die Kontrolle über ihre Personenstandsurkunden behalten und diese zur Identitätsprüfung verwenden können. Eine Voraussetzung dafür ist die sichere Verknüpfung des Dokuments mit seinem legitimen Inhaber.

Fazit: Herkömmliche Sterbeurkunden liegen bisher meist nur in Papierform vor, und deren Formate und Inhalte sind nicht länderübergreifend harmonisiert. Die europäische Standardisierung zur Definition von digitalen Personenstandsurkunden (Geburts-, Heirats- und Sterbeurkunden) ist in Arbeit, wird aber noch viele Jahre in Anspruch nehmen. Bis dahin bleiben die Prozesse der Ausstellung und Übermittlung von Sterbeurkunden uneinheitlich. Dienstanbieter haben bisher keinen direkten Zugriff auf die amtlichen Sterberegister. Für Dienstanbieter bleibt es schwierig, die Echtheit eingescannter Sterbeurkunden zu prüfen. Innerhalb der Europäischen Union lassen sich Sterbefälle mittels vorgeschriebener mehrsprachiger Formulare gut nachweisen.

7.4.2.2 Urkunden in einer Blockchain

Blockchains stellen eine mögliche Alternative zu klassischen Client-Server-Datenbanken dar. Im Vergleich zu Datenbanken können Blockchains Vorteile in Bezug auf Sicherheit und Verfügbarkeit bieten. So könnten viele Verwaltungsvorgänge und Auskunftsregister (wie Eigentumsnachweise, Zeugnisse, Organspende-, Heirats- oder Sterberegister) auf der Grundlage von Blockchains international transparent dokumentiert und so zum Schutz gegen Datenverlust und nachträgliche Manipulation eingesetzt werden. Weil Blockchains dezentrale Strukturen nutzen, kommen sie bevorzugt dann zum Einsatz, wenn keine zentrale Instanz gewünscht wird bzw. wenn zwischen den Teilnehmern weder hohes Vertrauen noch der Wille zur Bildung einer Hierarchie vorhanden sind. Durch den Einsatz von

Portugal, Schweiz, Spanien, Ungarn und Türkei. Deutschland war von 1956 bis 2015 Mitglied, akzeptiert aber weiterhin viele CIEC-Übereinkommen.

[60] *Brucker-Kley u. a.*, Sterben und Erben in der digitalen Welt: von der Tabuisierung zur Sensibilisierung, S. 68.

[61] Verordnung (EU) 2016/1191 des Europäischen Parlaments und des Rates vom 6. Juli 2016 zur Förderung der Freizügigkeit von Bürgern durch die Vereinfachung der Anforderungen an die Vorlage bestimmter öffentlicher Urkunden innerhalb der Europäischen Union und zur Änderung der Verordnung (EU) Nr. 1024/2012, Kapitel III.

[62] Die Spezifikation wird durch das europäische Standardisierungsgremium CEN/TC 224/WG 19 „Breeder Documents“ mit dem Arbeitstitel „Personal Identification – Secure and Interoperable European Breeder Documents“ erstellt.

Blockchains und den Verzicht auf eine zentrale Instanz für deren Betrieb erhofft man sich auch eine schnellere und günstigere Abwicklung von Transaktionen.

Blockchains beruhen auf sogenannten Distributed-Ledger-Technologien, die eine verteilte digitale Datenhaltung mit Eigenschaften ermöglichen, die in der herkömmlichen Buchführung wichtig sind. Die Technologien sichern insbesondere die Integrität und Authentizität der Daten. Dazu werden die Daten in einem Netzwerk gleichberechtigter Partner gehalten („Peer-to-Peer-Netzwerk“). Jeder Partner verwaltet eine lokale Kopie der gesamten Daten und kann selbst neue Daten hinzufügen. Die Partner entscheiden über einen kryptografisch gesicherten Konsensmechanismus gemeinsam über die Aktualisierung der Daten. Dieser Konsensmechanismus sorgt dafür, dass die verteilten Daten bei allen Partnern ohne eine zentrale Steuerung aktuell und konsistent bleiben. Die Regeln einer konkreten Blockchain sind in den Datensätzen selbst kodiert und werden automatisch in der Software durchgesetzt. Die einzelnen Datensätze sind als sogenannte Transaktionen validierbar und werden zu Datenblöcken zusammengefasst. Beim Hinzufügen eines neuen Datenblocks wird dieser mittels eines kryptografischen Hashverfahrens mit dem vorigen Datenblock verkettet, sodass die Reihenfolge und Inhalte der Transaktionen für alle nachvollziehbar festliegen. Die Abbildung 7.1 zeigt eine fiktive Blockchain mit Sterberegistereinträgen eines Netzwerks europäischer Standesämter.

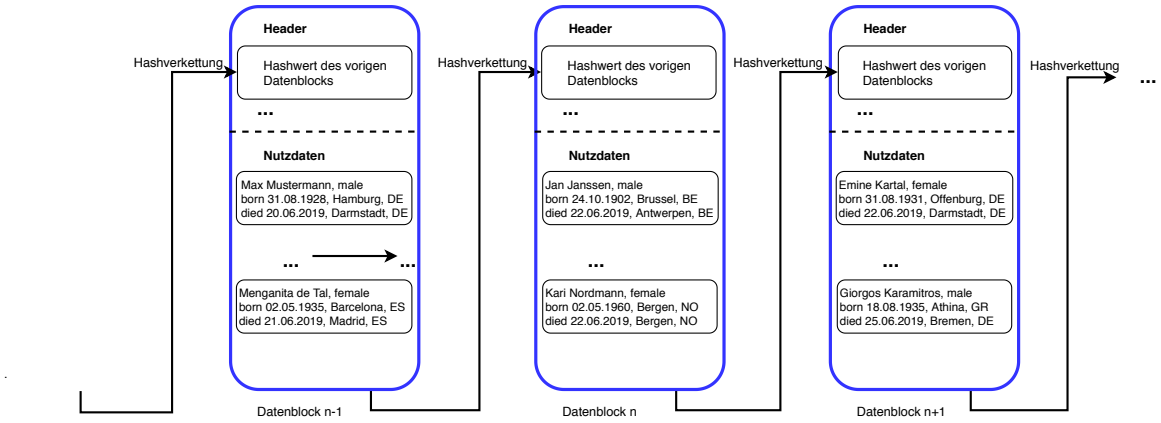

Abbildung 7.1: Sterberegister in Form einer Blockchain.

Zur Konzeption einer Blockchain müssen zunächst die gewünschten Eigenschaften in Form eines technischen Blockchain-Modells definiert werden, insbesondere der Zugriff auf das Netzwerk und auf die Daten. Soll das Schreiben und Lesen aller Daten uneingeschränkt zugelassen werden, so wäre dafür eine sogenannte öffentliche Blockchain („public blockchain“) geeignet. In einer öffentlichen, genehmigungsfreien Blockchain („permissionless blockchain“) dürfen grundsätzlich alle Teilnehmer die Datenblöcke validieren, neue Blöcke erzeugen und an der Konsensbildung teilnehmen. Im Gegensatz dazu hat eine sogenannte private Blockchain („private blockchain“) die Eigenschaft, nur bestimmten Nutzergruppen Zugriff auf Netzwerk und Daten zu gewähren. Eine zentrale Instanz ist nötig, um die Zugriffsrechte auf eine solche sogenannte genehmigungsbasierte Blockchain („permissioned blockchain“) zu regeln. Die in Abbildung 7.1 dargestellte Blockchain für Sterberegistereinträge würde sicherlich erfordern, dass nur die entsprechenden Standesämter über Schreibrechte verfügen. In Bezug auf die Schreibrechte würde es sich um eine private, genehmigungsbasierte Blockchain handeln. In Bezug auf die Leserechte wäre möglicherweise eine öffentliche, genehmigungsfreie Blockchain

denkbar, um international tätigen Dienstanbietern den einfachen Zugriff auf das Sterberegister zu ermöglichen.

Die für Blockchain charakteristische verteilte Datenhaltung macht in jedem Fall einen Konsensmechanismus unumgänglich, um die Übereinstimmung der verschiedenen Datenkopien sicherzustellen. Im Bereich der Konsensmechanismen wird die breite Diskussion von dem Verfahren „Proof-of-Work" (PoW) dominiert, das insbesondere wegen seines immensen Energiebedarfs in der Kritik steht. PoW ermöglicht es, die Daten ohne Authentisierung der einzelnen Parteien konsistent zu halten und dabei Manipulationen zu verhindern. Blockchains mit strikterer Rechtevergabe und Authentisierung der Parteien, wie sie z. B. für behördliche Auskunftsregister geboten scheinen, erlauben aber auch den Einsatz von sogenannten nachrichtenbasierten Konsensmechanismen, die wesentlich effizienter sind und deren Sicherheit gut untersucht ist.

Bei einem behördlichen Auskunftsregister wären somit entgegen der Grundidee der Blockchain eine oder mehrere zentrale Instanzen für die Vergabe und Durchsetzung von Zugriffsrechten zuständig. Damit werden die Blockchain-Vorteile der Dezentralität, Transparenz und Robustheit gegen Missbrauch teilweise wieder aufgegeben. Die Herkunft und Echtheit (Authentizität) der Einträge muss durch zusätzliche technische und organisatorische Infrastrukturmaßnahmen sichergestellt werden, z. B. mittels elektronischer Signatur der einzelnen Transaktionen durch das jeweils zuständige Standesamt.

Die rechtlichen Fragestellungen im Zusammenhang mit Blockchains resultieren unter anderem daraus, dass es keine zentrale, rechtlich verantwortliche Stelle im Regelbetrieb gibt. Daraus ergeben sich vielfältige Implikationen. Auch datenschutzrechtliche Probleme wie die Umsetzung von Vorgaben der DSGVO resultieren aus der auf Blockchains gerade erwünschten Transparenz und Manipulationssicherheit. Kontrovers wird diskutiert, ob eine datenschutzkonforme Gestaltung der Blockchain-Technologien überhaupt möglich ist. Die nicht veränderbare Rückverfolgbarkeit von Transaktionen einer personenbezogenen Blockchain kann dazu führen, dass die Betroffenenrechte gemäß DSGVO nur schwierig umgesetzt werden können, insbesondere die Rechte auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und Datenübertragbarkeit (Art. 20). Allerdings kommt die Form einer behördlich erstellten privaten Blockchain der Anwendbarkeit von Betroffenenrechten dadurch entgegen, dass eindeutig klar geregelt werden kann, welche Behörde für welche Einträge verantwortlich ist. Das BSI hat eine sicherheitstechnische und rechtliche Analyse der Blockchain-Technologie veröffentlicht.[63]

Fazit: Sterbeurkunden könnten in Form einer Blockchain zum Schutz gegen Datenverlust und nachträgliche Manipulation international verfügbar gemacht werden. Dazu müssten sich jedoch die Staaten auf ein bestimmtes Blockchain-Modell und auf die inhaltlichen Formate einigen. Zudem müssten die bisher sehr eingeschränkten Zugriffsrechte erweitert oder ein internationaler Auskunftsdienst (ähnlich dem deutschen Schufa-Dienst) eingerichtet werden, bei dem Dienstanbieter die von Nutzern gemeldeten Sterbefälle verifizieren können.

[63] *Berghoff u. a.*, Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen.

7.4.2.3 Rechtliche Bewertung

Die Vorlage einer Sterbeurkunde ist jedenfalls ein zuverlässigerer Beweis des Todesfalls als eine reine Bestätigung durch Vertrauenspersonen oder der Ablauf eines Zeitintervalls.

Die personenstandsrechtlichen Urkunden sind bisher jedoch nicht international harmonisiert, was grundsätzlich im Rahmen des Nachweises gegenüber ausländischen Anbietern Probleme bereiten kann. In diesem Zusammenhang ist allerdings die VO (EU) 2016/1191 vom 06. Juli 2016 zu beachten, nach der Personenstandsurkunden mehrsprachige Formulare beigefügt werden können. Außerdem ist Deutschland Vertragsstaat des CIEC-Übereinkommens Nr. 16 vom 8.9.1976 über die Ausstellung mehrsprachiger Auszüge aus Personenstandsurkunden. Somit besteht zumindest die Möglichkeit, durch das zuständige Standesamt einen mehrsprachigen Auszug aus dem Sterberegister ausstellen zu lassen, §§ 55 I Nr. 5, 60 PStG i. V. m. § 50 I, VII PStV, beispielsweise in englischer Sprache, § 50 II, III PStV. Dadurch soll die Verwendung von Personenstandsurkunden im Ausland erleichtert werden, indem keine gesonderte Übersetzung und in Vertragsstaaten für die Anerkennung keine weitere Legalisation, Beglaubigung oder ähnliche Förmlichkeiten mehr erforderlich sind.[64] Das Übereinkommen legt fest, dass den mehrsprachigen Auszügen dieselbe Beweiswirkung wie einer innerstaatlichen Urkunde zukommt.[65] Diese Urkunden werden auch als internationale Personenstandsurkunden bezeichnet.[66]

Hinsichtlich der Form der Personenstandsurkunden, also auch der Sterbeurkunde nach § 55 I Nr. 5 PStG, ist zu beachten, dass das Standesamt die in der Anlage zur Personenstandsverordnung festgelegten Formulare zu verwenden hat. Dadurch soll sichergestellt werden, dass die Urkunden als amtliches Dokument erkennbar sind und Fälschungen vorgebeugt wird,[67] also der Beweiswert der Urkunde gesichert wird. Dies gilt auch dann, wenn die Urkunde aus dem elektronischen Register ausgestellt wird.[68] Selbst wenn die Personenstandsurkunden in Form einer Blockchain gespeichert werden, wären aufgrund der gesetzlichen Regeln des Personenstandsregisters diese Formulare zu verwenden.

Zuständig für die Ausstellung von Personenstandsurkunden und damit auch von Sterbeurkunden sind ausschließlich die Standesämter, §§ 55 ff. PStG. Andere Institutionen sind nicht zur Ausstellung von Personenstandsurkunden befugt. Dies gilt auch für Gerichte oder Notare. Schreiberechte haben auch im Rahmen des elektronischen Personenstandsregisters nur die Standesämter. Dies würde auch für jedes andere elektronische Register gelten.

Daneben müsste auch das Einsichtsrecht in ein elektronisches Register beschränkt werden. Gemäß § 62 II, I 1 PStG ist auf Antrag den Personen Auskunft aus einem oder Einsicht in einen Registereintrag zu gewähren, auf die sich der Registereintrag bezieht, sowie deren Ehegatten, Lebenspartnern, Vorfahren und Abkömmlingen. Andere Personen haben diese Rechte nur, wenn sie ein rechtliches Interesse an dem Eintrag glaubhaft machen können, § 62 II, I 2 PStG. Somit besteht kein offener

[64] *Bornhofen*, in: Gaaz/Bornhofen (Hrsg.), Personenstandsgesetz Handkommentar, § 55 Rn. 15 f.
[65] *Bornhofen*, in: Gaaz/Bornhofen (Hrsg.), Personenstandsgesetz Handkommentar, § 54 Rn. 19.
[66] *Berkl*, Personenstandsrecht, Rn. 1097.
[67] *Berkl*, Personenstandsrecht, Rn. 1100.
[68] *Berkl*, Personenstandsrecht, Rn. 1105.

Zugang zu den Personenstandsregistern, sondern dieser wird nur einem begrenzten Kreis von Personen gewährt. Dies rechtfertigt sich aus den Regeln, die das BVerfG zum Schutz des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung aus Art. 2 I, 1 I GG aufgestellt hat. Ein unbeschränkter Zugang des Rechtsverkehrs zu den persönlichen Daten einer Person widerspricht diesem grundrechtlich garantierten Recht. Daher darf grundsätzlich jeder Einzelne selbst entscheiden, welche persönlichen Daten er im Rechtsverkehr preisgeben und verwenden will. Dies gilt insbesondere im Rahmen der modernen Datenverarbeitung, wo der Einzelne vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu schützen ist. Einschränkungen dieses Rechts muss der Einzelne nur bei überwiegendem Interesse der Allgemeinheit und wenn dies durch Gesetz bestimmt ist hinnehmen.[69] Unter welchen Voraussetzungen und wem Informationen aus dem Personenstandsregister erteilt werden, ist somit durch das Personenstandsgesetz abschließend geregelt. Auch die allgemeinen datenschutzrechtlichen Vorschriften sind insofern nachrangig.[70] Ein öffentlich zugängliches Register würde diesen Grundsätzen widersprechen.

Der Zugang zu einem digitalen Register könnte daher für nicht mit dem Betroffenen verwandte Personen nur bei Glaubhaftmachung eines rechtlichen Interesses gewährt werden. Zudem darf keine einfachere Möglichkeit der Rechtsverfolgung gegeben sein.[71] Das rechtliche Interesse ist gegeben, wenn die Kenntnis der Personenstandsdaten zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen erforderlich ist. Ein rechtliches Interesse setzt ein bereits bestehendes Recht voraus, das ohne die erstrebte Handlung in seinem Bestand gefährdet würde (Nr. 62.1.1 PStG-VwV). So wurde ein rechtliches Interesse zur Klärung einer tatsächlichen Unsicherheit über ein Rechtsverhältnis oder zum Erhalt einer sicheren Grundlage für die Verfolgung eines Anspruchs anerkannt.[72] Möchte der Dienstanbieter durch die Einsicht in das Sterberegister verifizieren, dass sein bisheriger Vertragspartner verstorben ist und damit der vertraglich geregelte Vorsorgefall eingetreten ist, könnte ein derartiges rechtliches Interesse jedoch wohl bejaht werden. Der Dienstanbieter möchte in diesem Fall durch die Einsicht in das Register feststellen, wer nun sein Vertragspartner ist und somit eine Unsicherheit über das Rechtsverhältnis beseitigen. Diese Voraussetzung wäre jedoch stets im Rahmen des Antrags auf Auskunft gegenüber dem zuständigen Standesamt im Einzelfall glaubhaft zu machen.

Da es sich um besonders sensible Daten handelt, müssen darüber hinaus bei dem Betrieb von elektronischen Registern besondere Sicherheitsanforderungen eingehalten werden. § 10 I PStV legt fest, dass für den Betrieb von Personenstandsregistern die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zu treffen sind, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen. Dabei dürfen nur Programme verwendet werden, die den anerkannten technischen Anforderungen an die maschinell geführte Verarbeitung von Daten mit hohem Schutzbedarf entsprechen.

[69] BVerfG, NJW 1984, 419 (422).
[70] *Bornhofen*, in: Gaaz/Bornhofen (Hrsg.), Personenstandsgesetz Handkommentar, § 61 Rn. 2; *Berkl*, Personenstandsrecht, Rn. 308.
[71] OLG Düsseldorf, FGPrax 2014, 40.
[72] *Berkl*, Personenstandsrecht, Rn. 324.

Nach § 10 II Nr. 1-9 PStV sind insbesondere die Zutritts-, Zugangs- und Zugriffskontrolle, Revisionssicherheit, Beweissicherung, Wiederaufbereitung, Unverfälschtheit, Verlässlichkeit und Übertragungssicherheit sicherzustellen. Weitere Sicherheitsanforderungen sind in den §§ 11 ff. PStV festgelegt.

Die Zurverfügungstellung von Sterbeurkunden in einer Blockchain würde diesen Anforderungen nicht genügen.

Da die Vorlage einer Sterbeurkunde gegenüber einem Dienstanbieter aber im Rahmen der vertraglichen Regelung Bedeutung erlangt, kann vereinbart werden, ob und in welcher Form diese vorzulegen ist. So kann zwar eine Vereinbarung dahingehend getroffen werden, dass eine englische Übersetzung der Sterbeurkunde vorzulegen ist. Genauso kann aber auch die Kopie oder ein Scan der deutschen Sterbeurkunde für ausreichend erklärt werden.

7.4.3 Vergleich und Bewertung der genannten Verfahren

Die folgende Tabelle 7.3 fasst die Lösungen der vorangegangenen Abschnitte anhand der am Anfang des Kapitels genannten Kriterien zusammen.

Lösung	Sicherheit	Datenschutz	Gebrauchstauglichk.
Einfache Bestätigungen	–	– –	++
Kryptograf. Lösungen	o	–	–
Herkömml. Sterbeurkunden	++	++	+
Blockchain-Sterbeurkunden	+	– –	++

Tabelle 7.3: Nachweismöglichkeiten über den Tod des Erblassers

Einfache Bestätigungen, d. h. die Konfiguration von Kontaktdaten der Vertrauenspersonen, die im Sterbefall automatisch benachrichtigt werden können, sind bereits Teil vieler Dienste zu digitalen Safes, siehe Kapitel 6.5.4 auf Seite 200. Diese umfassen aber in der Regel keine Prüfung von Sterbeurkunden. Kryptografische DeathSwitches könnten die Sicherheit von Bestätigungen verbessern, sind aber nur mit hohem Aufwand implementierbar. Herkömmliche eingescannte Sterbeurkunden werden vermutlich noch viele Jahre im Gebrauch sein, solange die amtlichen Verwaltungsprozesse nicht harmonisiert und grenzüberschreitend standardisiert sind. Sterbeurkunden in Form von Blockchains könnten die Verfügbarkeit und Integrität von Sterbeurkunden erhöhen, werfen aber Bedenken hinsichtlich des Datenschutzes auf. Entsprechend beschränkt beispielsweise die Vererbungsplattform PVDA (siehe Kapitel 6.5 auf Seite 192) den Zugriff auf Sterbeurkunden und andere personenbezogene Dokumente auf diejenigen Personen, die schon heute dazu autorisiert sind.[73]

Solange keine zentrale Verfügbarkeit von Nachlass- und Sterbeurkunden realisiert ist, könnten kleine und mittelständische Dienstanbieter ihren Kunden zur Vorsorge des digitalen Nachlasses Folgendes

[73] *Schmid u. a.*, Sterben im Internet – Regelung des digitalen Nachlasses, in: Wirtschaftsinformatik & Management 5.1, S. 86–96.

anbieten: Die Kunden können in ihren persönlichen Kontoeinstellungen die Kontaktdaten einer oder mehrerer Vertrauenspersonen hinterlegen und dazu auch die Weise festlegen, in der diese Kontaktperson(en) den Sterbefall mitteilen dürfen (z. B. persönlich vor Ort, telefonisch von einer bestimmten Festnetznummer, per E-Mail unter Vorlage einer eingescannten Sterbeurkunde). Besteht für den Dienstanbieter der Verdacht eines Sterbefalls, sieht er im betreffenden Nutzerkonto nach, wer zur Mitteilung des Sterbefalls berechtigt ist. Der Anbieter kontaktiert diese Person über die hinterlegten Kontaktdaten mit der Bitte um verbindliche Mitteilung in der vom Kontoinhaber festgelegten Form. Wurde der Sterbefall bestätigt, teilt der Dienstanbieter der Vertrauensperson ggf. mit, welche digitalen Werte mit dem Konto der verstorbenen Person verbunden sind.

Die folgende Tabelle 7.4 gibt einen Überblick über die Vor- und Nachteile der Nachweisverfahren über den Tod des Erblassers.

Tabelle 7.4: Nachweisverfahren über den Tod des Erblassers

Lösung	Vorteile	Nachteile
Einfache Bestätigung	✓ Feststellung von Inaktivität automatisch und einfach ✓ Kann von Kontoinhaber selbstbestimmt konfiguriert werden	✗ Erfordert vorab zusätzliche Prüfungen, um Falschmeldungen zu vermeiden ✗ Durch Einhaltung von Fristen keine Reaktion auf dringende Fälle möglich ✗ Jeder Anbieter müsste das implementieren ✗ Mit jedem Konto steigt der Aufwand bei Vertrauenspersonen ✗ Zusätzlicher Nachweis des Sterbefalls könnte notwendig sein
Kryptografisch unterstützte Bestätigung	✓ Feststellung von Inaktivität automatisch und einfach ✓ Kann von Kontoinhaber selbstbestimmt konfiguriert werden ✓ Bei gutem Design sicherer und zuverlässiger als einfache Bestätigung	✗ Komplexe Technologie, hoher Aufwand bei Dienstanbietern ✗ Hoher Aufwand bei Vertrauenspersonen ✗ Unzuverlässig, wenn zusätzliche Software und Passwörter nötig sind ✗ Zusätzlicher Nachweis des Sterbefalls könnte notwendig sein
Herkömmliche Sterbeurkunden	✓ Zuverlässiger Beweis des Todesfalls	✗ Personenstandsrechtliche Urkunden noch nicht international harmonisiert ✗ Nur Standesämter dürfen die Urkunden ausstellen ✗ Einsichtsrecht hat nur ein begrenzter Personenkreis

Fortsetzung auf der nächsten Seite

Tabelle 7.4: Nachweisverfahren über den Tod des Erblassers (Fortsetzung)

Lösung	Vorteile	Nachteile
Urkunden in einer Blockchain	✓ Integrität, Verfügbarkeit und Transparenz der Daten auch international möglich ✓ Schnelle und günstige Veröffentlichung möglich	✗ Datenschutz schwierig zu realisieren ✗ Für Einsicht wäre „Glaubhaftmachung eines rechtlichen Interesses“ ebenso gefordert ✗ Erfüllt die Sicherheitsanforderungen an elektronische Register nicht ✗ Viele technische, rechtliche und organisatorische Fragen ungeklärt

7.5 Nachweismöglichkeiten über den Eintritt der Hilfsbedürftigkeit

Ist die vertragliche Vorsorge für den Fall der Hilfsbedürftigkeit getroffen, hängt die Frage, ob der Eintritt der Hilfsbedürftigkeit nachgewiesen werden muss, von der vertraglichen Regelung ab.

Generell gilt für den Fall der Vorsorgevollmacht, dass für die Feststellung, ob der Vollmachtgeber tatsächlich hilfsbedürftig ist, kein geregeltes Verfahren wie im Betreuungsverfahren existiert, was zu praktischen Schwierigkeiten bei Gebrauch der Vollmacht führen kann, wenn diese im Außenverhältnis nur für den Fall der Hilfsbedürftigkeit (bedingt) erteilt ist.[74] Aus diesem Grund ist auch im Fall der in Kapitel 7.2.1.3 auf Seite 294 vorgeschlagenen vertraglichen Regelung die Wirksamkeit der Stellvertretung nicht durch den Eintritt der Hilfsbedürftigkeit bedingt. Zwar wäre grundsätzlich denkbar, dass die Bevollmächtigung insofern bedingt erteilt ist, als sie erst wirksam wird, wenn der Stellvertreter gegenüber dem Dienstanbieter den Eintritt der Hilfsbedürftigkeit nachweist. Allerdings könnte dies – zum Nachteil des Verbrauchers – zu Beweisschwierigkeiten und vor allem bei zeitlich sensiblen Rechtshandlungen zu Verzögerungen führen. Auch sonst wird daher für Vorsorgevollmachten empfohlen, dass diese im Außenverhältnis unbedingt (also mit sofortigem Eintritt der Wirksamkeit) erteilt werden, sodass der Eintritt der Hilfsbedürftigkeit gegenüber Geschäftspartnern nicht nachzuweisen ist. Der Zeitpunkt des Gebrauchs der Vollmacht ist nur im Innenverhältnis zwischen Vollmachtgeber und -nehmer geregelt, auf die Wirksamkeit im Außenverhältnis hat dies keine Auswirkungen.[75]

Dies sollte auch im Rahmen der vertraglich vorgesehenen Benennung eines Stellvertreters gelten. Es ist zwar zuzugeben, dass dann die Gefahr eines verfrühten Gebrauchs der Vollmacht durch den Stellvertreter besteht, wobei das Risiko der Verbraucher trägt. Allerdings erfordert die Erteilung einer Vorsorgevollmacht unter diesen Voraussetzungen stets ein gewisses Vertrauen des Vollmachtgebers in seinen Stellvertreter, dass dieser die Stellvertretung nicht missbräuchlich ausübt. Zudem können

[74] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 58; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 246.

[75] *Schneider*, in: Säcker u. a. (Hrsg.), MükoBGB, § 1896 Rn. 59; *Schmidt-Recla*, in: Gsell u. a. (Hrsg.), BeckOGK BGB, § 1896 Rn. 248.

hier konkrete Anweisungen im Innenverhältnis zum Gebrauch der Vollmacht erteilt werden und für den Fall der Zuwiderhandlung der Widerruf der Vollmacht angedroht werden.

Auf diese Risiken ist der Verbraucher – auch zur Wahrung des Transparenzgebots, § 307 I 2 BGB – allerdings ausdrücklich hinzuweisen.

Die Dienstanbieter sind insofern vor einer Haftung in der Regel dadurch geschützt, dass durch die Benennung des Stellvertreters ihnen gegenüber ein Rechtsscheintatbestand für das Bestehen der Vollmacht vorliegt. Die Verbraucher könnten durch die Dienstanbieter zusätzlich dadurch geschützt werden, dass sie – beispielsweise über die im Nutzerkonto hinterlegte E-Mail-Adresse – stets benachrichtigt werden, wenn eine neue Anmeldung bei dem Nutzerkonto erfolgt. So könnte der Verbraucher unverzüglich Kenntnis davon erlangen, wenn der Stellvertreter sich in das Konto einloggt und gegebenenfalls einschreiten. Dies könnte erfolgen, indem der Verbraucher in der zugesendeten E-Mail darauf hingewiesen wird, dass eine neue Anmeldung erfolgt ist. Falls der Verbraucher sich auf diese E-Mail nicht zurückmeldet, darf der Dienstanbieter vermuten, dass entweder der Vorsorgefall eingetreten ist, oder dass der Verbraucher das Verhalten des Stellvertreters billigt. Möchte der Verbraucher den weiteren Zugriff des Stellvertreters unterbinden, müsste er auf die E-Mail des Dienstanbieters reagieren. In diesem Fall wäre das Nutzerkonto zu sperren. Diesbezüglich wäre sinnvoll, dass der Stellvertreter einen eigenen Zugang in Form eines zweiten Satzes Zugangsdaten erhält, mit dem er sich selbstständig in das Nutzerkonto des Vollmachtgebers einloggen kann. Dann würde im Fall des Missbrauchs der Vollmacht nur der Zugang des Stellvertreters gesperrt und nicht das gesamte Nutzerkonto des Vollmachtgebers. Allerdings könnte dies wohl auch ohne gesonderten Zugang des Stellvertreters dadurch gelöst werden, dass dem Vollmachtgeber im Fall der Sperrung des Nutzerkontos zeitgleich die Möglichkeit eröffnet wird, das Passwort zu ändern, um so einen weiteren Zugriff des Stellvertreters zu verhindern.

Etwas anderes könnte jedoch gelten, wenn vertraglich für den Eintritt der Hilfsbedürftigkeit die Löschung des Kontos vorgesehen ist. Hier muss der Dienstanbieter in zumutbarer Weise vom Eintritt des Vorsorgefalls erfahren, um die vertragliche Regelung umsetzen zu können. Denkbar ist hier zunächst, dass eine Vertrauensperson den Eintritt der Hilfsbedürftigkeit mitteilt und auf diese Mitteilung hin eine Löschung des Kontos erfolgt. Diesbezüglich ist jedoch zu beachten, dass dies zwar eine einfache Möglichkeit ist, bei einer falschen Mitteilung und daraufhin erfolgten (ordnungsgemäßen) Löschung die Daten aber – wohl unwiederbringlich – verloren sind. Daher könnte in diesem Fall ein berechtigtes Interesse dahingehend bestehen, dass nicht nur eine Vertrauensperson gegenüber dem Dienstanbieter zu benennen ist, die den Eintritt der Hilfsbedürftigkeit mitteilt, sondern dass dies zusätzlich durch ein ärztliches Attests (ggf. als Kopie oder Scan) nachzuweisen ist. Allerdings sind in diesem Fall die Voraussetzungen für das ärztliche Attest eindeutig und unmissverständlich festzulegen. Meldet sich die Vertrauensperson nicht, kann in diesem Fall eine Löschung dann erfolgen, wenn ein dem Dienstanbieter unbekannter Vorsorgebevollmächtigter durch Vorlage der Vollmachtsurkunde Zugriff auf das Konto begehrt. Auch wenn die Vorsorgevollmacht umfassend erteilt wurde und grundsätzlich den Zugriff auf das Nutzerkonto umfassen würde, hat die Löschung zu erfolgen, da die vertragliche Regelung insoweit vorgeht. In diesem Fall darf der Dienstanbieter vermuten, dass der Vorsorgefall eingetreten ist. Hilfsweise kann auch hier festgelegt werden, dass das Konto nach dem

Ablauf eines längeren Zeitraums der Inaktivität gelöscht wird. Insofern ist jedoch eine Warnung des Nutzers über die Löschung vorzusehen.

7.6 Zusammenfassung

Eine vertragliche Vorsorge ist sowohl für den Fall des Todes als auch des Eintritts der Handlungsunfähigkeit des Nutzers möglich. Aus Verbrauchersicht ist dies auch sinnvoll, da sich bei einer Einbeziehung des Dienstanbieters in die Vorsorge weniger Probleme hinsichtlich der Legitimation stellen und so dem Willen des Verbrauchers Geltung verschafft werden kann. Zur praktischen Umsetzung einer solchen vertraglichen Regelung kann der Dienstanbieter den Verbrauchern verschiedene Vorsorgemöglichkeiten zur Verfügung stellen und so bei der Vorsorge unterstützend tätig werden. Allerdings sind für die Wirksamkeit einer solchen vertraglichen Regelung unter anderem die Voraussetzungen des Transparenzgebots einzuhalten. Dem Verbraucher ist somit hinreichend klar, verständlich und eindeutig vor Augen zu führen, welche Rechtswirkungen durch seine Erklärung ausgelöst werden. Auch ist in jedem Fall erforderlich, dass es dem Verbraucher offen steht, ob die Vorsorge durch eine vertragliche Regelung oder durch eigenständige Vorsorge mittels letztwilliger Verfügung oder Vorsorgevollmacht erfolgen soll.

Die vertragliche Vorsorge ist jedenfalls durch eine Konfiguration der Dienste technisch zu unterstützen und kann durch weitere technische Mittel begleitet werden. Dazu wurden verschiedene technisch-organisatorische Umsetzungsmöglichkeiten untersucht. Eine Erweiterung der Passwort-Vergessen-Funktion um das sofortige Neusetzen der E-Mail-Adresse (Benutzername) und der Sicherheitsantworten zusätzlich zum neuen Passwort würde zusätzliche Sicherheitsmaßnahmen erfordern, die aufseiten der Nutzer Kosten verursachen und die Übergabe der Nutzerkonten an Begünstigte komplizierter machen.

Die Integration von SSO-Diensten (z. B. Plugin für den Facebook-Login) mit dem Ziel, Begünstigten des digitalen Nachlasses den Zugriff auf das Konto des Erblassers zu gewähren, erweitert die Vorsorgemöglichkeiten des digitalen Nachlasses, ist allerdings hinsichtlich Datenschutz und Sicherheit fragwürdig. Denkbar ist ein SSO-Login über den deutsch-europäischen Identitätsdienst Verimi. Allerdings muss hierzu einerseits der Dienstanbieter, bei dem der Login erfolgen soll, mit dem Dienst Verimi kooperieren. Zudem muss der jeweilige Begünstigte über ein Nutzerkonto bei Verimi verfügen. Eine derartige Anmeldung sollte auf der freien Entscheidung des Verbrauchers beruhen, insbesondere, da auch im Rahmen von Verimi eine Datenspeicherung erfolgt.

Die erweiterten Konfigurationsmöglichkeiten der Nutzerkonten für den digitalen Nachlass, wie ihn einige Online-Dienste wie Google und Facebook bereits anbieten, haben den Vorteil, dass Nutzer selbstbestimmt vorsorgen und den Nachlass klar regeln können. Allerdings sind es Lösungen, die von den Dienstanbietern vorgegeben sind. Andererseits kann eine solche Konfiguration umfassende Qualität bieten, weil der Dienstanbieter selbst das Interesse daran hat, dass systemeigene Funktionen auch gut funktionieren. Dafür muss allerdings der Anbieter zunächst ein grundsätzliche Interesse daran

haben, die Möglichkeiten des digitalen Nachlasses für den Nutzer zu verbessern. Hat ein Kontoinhaber die Kontaktdaten von Vertrauenspersonen (deren E-Mail-Adressen, Telefonnummern) in seinem Nutzerkonto hinterlegt, so kann die Nutzung dieser Daten im Bedarfsfall für den Dienstanbieter ein zuverlässiger Hinweis sein, dass die genannte Vertrauensperson wirklich online anwesend ist. Hinterlegte Kontaktdaten würden den Dienstanbietern relativ sichere und einfache Möglichkeiten bieten, mit den Begünstigten zu kommunizieren und ihnen die Ausübung ihrer Rechte zu ermöglichen.

Auch aus Nutzersicht sind solche Konfigurationsmöglichkeiten relativ einfach und preisgünstig, da die Voraussetzungen dafür meist erfüllt sind. Die Verfahren könnten sich relativ schnell verbreiten und sind bei vielen Diensten zumindest in Ansätzen bereits realisiert. Allerdings können bei einer zunehmenden Speicherung von Kontaktdaten (über die Daten des Kontoinhabers hinaus) Datenschutzfragen verstärkt in den Vordergrund rücken. Eine zweckfremde Nutzung der hinterlegten Kontaktdaten zur Datenerhebung, zur Kundenbefragung oder zur Zusendung von E-Mails mit anderem Inhalt ist den Dienstanbietern vertraglich zu untersagen.

Um die Dienstanbieter in die Übergabe des digitalen Nachlasses einzubeziehen, muss es zudem Maßnahmen geben, wie die Dienstanbieter die Information über einen Sterbefall aus einer zuverlässigen Quelle erhalten. Daher wurden auch technisch-organisatorische Nachweismöglichkeiten über den Tod des Erblassers untersucht. So können die vom Kontoinhaber hinterlegten Kontaktdaten von Vertrauenspersonen dazu genutzt werden, um nach einer vereinbarten Frist ohne Nutzeraktivität automatische Nachrichten an die Vertrauenspersonen zu senden mit der Bitte, den vermuteten Sterbefall zu bestätigen. Dies sollte allerdings so konfigurierbar sein, dass mehrere Vertrauenspersonen einbezogen werden müssen. Ein bloßes Ausbleiben der Online-Aktivitäten des Erblassers darf für den Dienstanbieter kein hinreichender Grund sein, den Zugriff auf persönliche Daten des Kontoinhabers für andere Personen freizuschalten. Lösungen, bei den die Antworten der Kontaktpersonen zudem kryptografisch verknüpft werden, könnten mehr Sicherheit und Datenschutz bieten, sodass eine versehentliche Freigabe der Daten unwahrscheinlicher wird. Der Aufwand ist aber sowohl aufseiten der Dienstanbieter als auch auf Nutzerseite sehr hoch.

Die Verwendung herkömmlicher Sterbeurkunden scheint naheliegend, ist jedoch nicht trivial, da die Ausstellung und Übermittlung von Sterbeurkunden noch nicht länderübergreifend harmonisiert ist. Für Dienstanbieter bleibt es schwierig, die Echtheit eingescannter Sterbeurkunden zu prüfen. Zudem haben sie keinen direkten Zugriff auf amtliche Sterberegister. Denkbar ist es, dass Sterbeurkunden in Form einer Blockchain international verfügbar gemacht werden. Dazu müssten aber die bisher sehr eingeschränkten Zugriffsrechte erweitert werden. Da es sich um besonders sensible Daten handelt, müssen für jedes elektronische Sterberegister besondere Sicherheitsanforderungen eingehalten werden. Die Zurverfügungstellung von Sterbeurkunden in einer Blockchain würde diesen Anforderungen nicht genügen. Da die Vorlage einer Sterbeurkunde gegenüber einem Dienstanbieter aber im Rahmen der vertraglichen Regelung Bedeutung erlangt, kann vereinbart werden, ob und in welcher Form diese vorzulegen ist.

So kann zwar eine Vereinbarung dahingehend getroffen werden, dass die Sterbeurkunde sowie ein mehrsprachiges Formular i. S. d. VO (EU) 2016/1191 vom 6. Juli 2016 vorzulegen ist. Genauso kann

aber auch die Kopie oder ein Scan der Sterbeurkunde in deutscher Sprache für ausreichend erklärt werden.

Das Wichtigste in Kürze

- Ein Verbraucher kann vertraglich mit einem Dienstanbieter vereinbaren, was nach seinem Tod mit einem Nutzerkonto geschehen soll. Dabei kann grundsätzlich entweder eine Löschung oder eine Übertragung des Nutzerkontos festgelegt werden. Immer hat der Verbraucher aber die Alternative, gar keine Regelung zu treffen.

- Ein Verbraucher kann daneben vertraglich mit einem Dienstanbieter vereinbaren, was in dem Fall mit seinem Nutzerkonto geschehen soll, wenn er sich aus gesundheitlichen Gründen nicht mehr selbst darum kümmern kann. Auch hier kann eine Löschung oder eine Verwaltung des Nutzerkontos durch einen Stellvertreter vereinbart werden, oder festgelegt werden, dass gar keine Regelung erfolgen soll.

- Um dies umzusetzen, können Vertrauenspersonen gegenüber dem Dienstanbieter benannt werden, die entweder nur den Eintritt des Vorsorgefalls bestätigen oder dann auf das Nutzerkonto zugreifen können.

- Ob und welche Nachweise hierfür erforderlich sind, kann vertraglich vereinbart werden. Der Dienstanbieter hat zwar ein Interesse daran, nicht einer falschen Person oder einer Person zu einem falschen Zeitpunkt Zugang zu einem Nutzerkonto zu gewähren. Aus Verbrauchersicht sollten aber auch keine zu hohen Anforderungen an den Nachweis gestellt werden.

8 Zielgruppenspezifische Empfehlungen

8.1 Empfehlungen für Erblasser und Erben

An Erblasser und Erben können folgende Empfehlungen gerichtet werden:

EE 1: Den Erblassern wird empfohlen, eine letztwillige Verfügung zu errichten, die auch regelt, was nach ihrem Tod mit dem digitalen Nachlass geschehen soll.
Für Details zu dieser Empfehlung siehe Kapitel 6.4 auf Seite 181.

EE 2: Daneben wird den Erblassern empfohlen, in einem von der letztwilligen Verfügung getrennten Dokument die Namen ihrer Online-Nutzerkonten mitsamt den Zugangsdaten aufzulisten und diese Liste aktuell zu halten.[1] Dazu sollten separat auf Papier die Anweisungen, was im Sterbefall mit der Liste zu tun ist (einschließlich Beschreibung des Aufbewahrungsort der Liste) zusammengestellt und zugänglich aufbewahrt werden. Die Liste kann digital mithilfe eines sicheren Passwort-Manager-Programms (z. B. KeePass) geführt werden. Auf diese Weise kann eine lokale verschlüsselte Passwortdatenbank (z. B. auf einem USB-Stick) angelegt und ein Notfalldatenblatt ausgedruckt werden, das den Anweisungen hinzugefügt werden sollte.
Für Details zu dieser Empfehlung siehe Kapitel 6.5.3 auf Seite 196 und 6.5.8 auf Seite 217.

EE 3: Im Regelfall sind Erben befugt, Online-Nutzerkonten des Erblassers wie dieser selbst zu benutzen. Etwas anderes gilt nur, wenn dies durch Anordnungen des Erblassers in seiner letztwilligen Verfügung festgelegt ist. Erben dürfen daher die Nutzerkonten einsehen, aktiv weiterführen (z. B. indem sie über einen E-Mail-Account des Erblassers Nachrichten schreiben oder das Onlinebanking-Portal weiternutzen) und Online-Vertragsverhältnisse kündigen. Allerdings müssen die Erben jedenfalls bei der Weiternutzung eines auf die Person des Erblassers bezogenen E-Mail- oder Social-Media-Accounts die Profilseite an ihre Person anpassen oder einen entsprechenden Nachfolgehinweis dahingehend erteilen, dass nicht mehr der Erblasser, sondern die Erben nun das Konto nutzen.
Für Details zu dieser Empfehlung siehe Kapitel 2.3.2 auf Seite 43.

EE 4: Sofern rechtlich zulässig, wird den Erben empfohlen, alle ihnen bekannten E-Mail-Postfächer des Erblasser für einen Zeitraum von ca. 3–5 Jahren weiter abzurufen, um über bevorstehende Deaktivierungen von ihnen bis dahin nicht bekannten Nutzeraccounts des Erblassers Kenntnis

[1] In Bezug darauf, die Liste aktuell zu halten, kann den Verbrauchern zusätzlich empfohlen werden, ihren digitalen Nachlass regelmäßig „aufzuräumen“. Hiermit ist insbesondere gemeint, Nutzeraccounts, die ein Verbraucher zukünftig nicht mehr nutzen möchte, schließen und ggf. die beim Dienstanbieter hinterlegten Daten löschen zu lassen.

nehmen zu können.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.5 auf Seite 167.

EE 5: Wollen die Erben gegenüber einem Online-Dienstanbieter ihre Rechte geltend machen, ist der Dienstanbieter über den Erbfall zu informieren. Auf Verlangen des Dienstanbieters müssen sich die Erben gegenüber diesem auch legitimieren.
Für Details zu dieser Empfehlung siehe Kapitel 6.6 auf Seite 231.

8.2 Empfehlungen für Vollmachtgeber, Vorsorgebevollmächtigte und Betreuer

An Vollmachtgeber, Vorsorgebevollmächtigte und Betreuer können folgende Empfehlungen gerichtet werden:

VB 1: Verbrauchern wird empfohlen, für den Fall, dass sie sich aus gesundheitlichen Gründen nicht mehr selbst um ihre Angelegenheiten kümmern können, eine Vorsorgevollmacht zu errichten, die auch den digitalen Bereich umfasst.
Für Details zu dieser Empfehlung siehe Kapitel 6.2 auf Seite 176.

VB 2: Daneben sollten die Namen der Online-Nutzerkonten mitsamt den Zugangsdaten aufgelistet und die Liste aktuell gehalten werden.[2] Dazu sollten separat auf Papier die Anweisungen, was im Vorsorgefall mit der Liste zu tun ist (einschließlich Beschreibung des Aufbewahrungsort der Liste) zusammengestellt und zugänglich aufbewahrt werden. Die Liste kann digital mithilfe eines sicheren Passwort-Manager-Programms (z. B. KeePass) geführt werden. Auf diese Weise kann eine lokale verschlüsselte Passwortdatenbank (z. B. auf einem USB-Stick) angelegt und ein Notfalldatenblatt ausgedruckt werden, das den Anweisungen hinzugefügt werden sollte. Dies kann auch empfohlen werden, um einem Betreuer einen Überblick über vorhandene Nutzerkonten zu verschaffen und diesem den Zugriff auf Nutzerkonten zu erleichtern.
Für Details zu dieser Empfehlung siehe Kapitel 6.5.3 auf Seite 196 und 6.5.8 auf Seite 217.

VB 3: Hinsichtlich der Bestellung eines Betreuers sollte darauf geachtet werden, dass sein Aufgabenkreis auch sämtliche relevanten digitalen Angelegenheiten umfasst. So sollte insbesondere der Aufgabenkreis Vermögenssorge nicht zu eng gefasst sein, damit – falls erforderlich – nicht nur klassische Bankgeschäfte, sondern auch die Verwaltung von Nutzerkonten bei Online-Bezahldiensten oder Kryptowährungen umfasst sind.
Für Details zu dieser Empfehlung siehe Kapitel 3.2.1 auf Seite 54.

VB 4: Kann oder will die betroffene Person nicht in die Durchsicht ihrer (digitalen) Post durch den Betreuer einwilligen, kann gerichtlich die Kontrolle des Post- und Fernmeldeverkehrs angeordnet werden. Diese Anordnung umfasst als Annexkompetenz zum Aufgabenkreis des Betreuers auch die digitale Kommunikation der betroffenen Person. In diesem Zusammenhang ist der Betreuer befugt, in Nutzerkonten der betroffenen Person Einsicht zu nehmen, allerdings nur, soweit dies zur Erfüllung seines Aufgabenkreises erforderlich ist. So kann der Zugriff auf bestimmte Nutzerkonten gänzlich verweigert werden, wenn diese keinen Zusammenhang zum Aufgabenkreis des Betreuers aufweisen. Die Selbstbestimmung der betroffenen Person ist so weit wie möglich zu gewährleisten. Handelt es sich aber um ein Nutzerkonto, über das sowohl private als auch geschäftliche Kommunikation geführt wird, darf sich der Betreuer zunächst Zugang zu dem Nutzerkonto verschaffen. Der Betreuer hat dann im Rahmen sachgemäßer

[2] In Bezug darauf, die Liste aktuell zu halten, kann den Verbrauchern zusätzlich empfohlen werden, ihren digitalen Nachlass regelmäßig „aufzuräumen“. Hiermit ist insbesondere gemeint, Nutzeraccounts, die ein Verbraucher zukünftig nicht mehr nutzen möchte, schließen und ggf. die beim Dienstanbieter hinterlegten Daten löschen zu lassen.

Prüfung zu beurteilen, ob eine über dieses Nutzerkonto empfangene Nachricht im Einzelfall seinen Aufgabenkreis betrifft.
Für Details zu dieser Empfehlung siehe Kapitel 3.3.1.1 auf Seite 59.

VB 5: Die Befugnisse zur Post- und Fernmeldekontrolle können auch einem Vorsorgebevollmächtigten durch die Vorsorgevollmacht übertragen werden. Auch der Vorsorgebevollmächtigte darf somit eigenständig in Nutzerkonten des Vollmachtgebers Einsicht nehmen. In diesem Zusammenhang ist dem Vollmachtgeber zu empfehlen, die Befugnis des Bevollmächtigten zur Fernmeldekontrolle in der Vorsorgevollmacht ausdrücklich anzuordnen, wenn er diese wünscht.
Für Details zu dieser Empfehlung siehe Kapitel 3.3.1.3 auf Seite 65.
Für einen Formulierungsvorschlag zu dieser Empfehlung siehe Kapitel 9 auf Seite 345.

VB 6: Soweit dies zur Erfüllung seines Aufgabenkreises erforderlich ist, ist ein Betreuer befugt, Nutzerkonten der betroffenen Person zu nutzen. Die aktive Nutzung muss dabei nicht als eigene Aufgabe an den Betreuer übertragen werden, da es sich um eine notwendige Kompetenz zur Erfüllung des Aufgabenkreises handelt. Auch ein Vorsorgebevollmächtigter kann Nutzerkonten des Vollmachtgebers aktiv nutzen, wenn er hierzu durch die Vollmacht ermächtigt wurde. In diesem Zusammenhang haben sich sowohl Betreuer als auch Vorsorgebevollmächtigte am (mutmaßlichen) Willen und Interesse des Nutzers zu orientieren.
Um Irrtümer oder Täuschungen im Rechtsverkehr zu vermeiden, hat der Stellvertreter gegenüber den Kommunikationspartnern des Verbrauchers die Stellvertretungssituation kenntlich zu machen. Es kann entweder gegenüber dem jeweiligen Kommunikationspartner eine generelle Erklärung abgegeben werden, dass Nachrichten von dem betreffenden Nutzerkonto zukünftig von dem Vertreter verfasst werden. Alternativ kann in jeder einzelnen Nachricht ein Hinweis darauf erfolgen, dass ein Vertreter für den Verbraucher tätig wird.
Für Details zu dieser Empfehlung siehe Kapitel 3.3.2 auf Seite 69.

VB 7: Die Kündigung eines Online-Vertragsverhältnisses kann dann vom Aufgabenkreis eines Betreuers umfasst sein, wenn dies zum Wohle der fürsorgebedürftigen Person erforderlich ist. Eine Kündigung kann im Rahmen der Vermögenssicherungs- und Vermögenserhaltungspflicht angezeigt sein, wenn die Vertragsdurchführung mit Kosten verbunden ist, die die Mittel der betroffenen Person übersteigen oder diese nicht mehr in der Lage ist, den Dienst zu nutzen.
Für Details zu dieser Empfehlung siehe Kapitel 3.3.3 auf Seite 76.

VB 8: Wird ein Stellvertreter für den Verbraucher gegenüber einem Online-Dienstanbieter tätig, ist der Dienstanbieter über diesen Umstand zu informieren. Auf Verlangen des Dienstanbieters hat der Stellvertreter seine Vertretungsbefugnis nachzuweisen.
Für Details zu dieser Empfehlung siehe Kapitel 6.6 auf Seite 231.

8.3 Empfehlungen für Unternehmen

An Dienstanbieter können folgende Empfehlungen gerichtet werden:

U 1: Den Dienstanbietern wird empfohlen, ihre Dienstnutzer in angemessener – d. h. in kurzer und allgemeinverständlicher – Form über deren Rechte in Bezug auf das digitale Erbe aufzuklären. Ggf. können sich Dienstanbieter hierfür ein Beispiel am sogenannten „Datenschutz-Steckbrief“ nehmen und einen „Steckbrief zum digitalen Nachlass“ entwickeln.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.2 auf Seite 164.

U 2: Mehr Transparenz in den AGB können Dienstanbieter u. a. dadurch erreichen, dass sie Regelungen zum digitalen Nachlass durch eine entsprechende Überschrift kennzeichnen und AGB-Klauseln, die den Ausschluss einer Guthabenübertragung an Dritte o. ä. betreffen, deutlich hervorheben. Auch sollte klargestellt werden, ob Erben, Vorsorgebevollmächtigte und Betreuer „Dritte“ im Sinne der relevanten Klauseln sein sollen.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.3 auf Seite 166.

U 3: Dienstanbietern – insbesondere Anbietern sozialer Netzwerkplattformen – kann empfohlen werden, den Verbrauchern über die AGB eine Wahlmöglichkeit in Bezug auf ihren digitalen Nachlass einzuräumen, sodass sie z. B. zu Lebzeiten wählen können, dass ihr Account in ihrem Todesfall gelöscht werden soll, ohne dass Erben (vorher) Zugriff auf diesen erhalten. Zugunsten der Verbraucher sollten die entsprechenden AGB-Klauseln so formuliert sein, dass die von dem Erblasser getätigte Wahl für den Dienstanbieter rechtsverbindlich ist und die Umsetzung nicht nur im vertraglich festgelegten Ermessen des Dienstanbieters liegt.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.6 auf Seite 168.

U 4: Diese Wahlmöglichkeit kann durch ein Optionsrecht für die Verbraucher umgesetzt werden. Es sollten nicht nur Wahlmöglichkeiten für den Sterbefall, sondern auch für den Fall des Eintritts der Handlungsunfähigkeit vorgesehen werden, indem beispielsweise die Möglichkeit eröffnet wird, einen Stellvertreter gegenüber dem Dienstanbieter zu benennen.
Für Details zu dieser Empfehlung siehe Kapitel 7.2.1 auf Seite 292 und 7.2.2 auf Seite 298

U 5: Das Einräumen einer Wahlmöglichkeit zum digitalen Nachlass des Verbrauchers sollte zusätzlich technisch durch Konfigurationsmöglichkeiten des Nutzerkontos unterstützt werden, um den Verbraucher in die Lage zu versetzen, aus den verschiedenen Nachlassoptionen die gewünschte Option für sein Nutzerkonto festzulegen. Neben der Löschung des gesamten Nutzerkontos wären die Archivierung der Daten zur Ansicht und die vollständige Übergabe des Nutzerkontos an die Erben sinnvolle Optionen. Für verschiedene Daten des Nutzerkontos sollte ein unterschiedlicher Umgang im digitalen Nachlass festgelegt werden können, beispielsweise, dass die Erben Zugriff auf sämtliche Fotos, nicht aber auf sonstige Beiträge, erhalten sollen, oder dass E-Mails zwar angesehen, aber nicht mehr neu im Namen des Erblassers geschrieben werden dürfen. Die Konfiguration des Nutzerkontos sollte aber auch zulassen, dass der Nutzer sich an dieser Stelle auf keine Regelung festlegt.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.6 auf Seite 168 und 7.3.2 auf Seite 305.

U 6: Die Konfiguration des Nutzerkontos sollte den Eintrag von mehreren Vertrauenspersonen zulassen, deren Kontaktdaten (E-Mail-Adresse, Telefonnummer) ausschließlich dem Zweck des digitalen Nachlasses dienen dürfen, beispielsweise damit der Dienstanbieter nach einer Inaktivitätsfrist des Kontoinhabers die Personen kontaktieren und einen vermeintlichen Sterbefall bestätigen lassen kann.
Für Details zu dieser Empfehlung siehe Kapitel 7.4.1 auf Seite 317.

U 7: Eine bevorstehende Deaktivierung eines Nutzeraccounts sollte der Dienstanbieter dem Dienstnutzer – und somit in dessen Todesfall ggf. auch seinen Erben – rechtzeitig (per E-Mail) angezeigt werden. Auch im Hinblick auf die Erben sollte die erstmalige Information über die bevorstehende Deaktivierung nach Möglichkeit bereits ca. 21 Tage vor der Deaktivierung erfolgen.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.5 auf Seite 167.

U 8: An den Nachweis der Legitimation der gegenüber dem Dienstanbieter benannten Personen, Stellvertreter und Rechtsnachfolger sollten im Rahmen der vertraglichen Regelung keine zu hohen Anforderungen geknüpft werden. Werden Legitimationsnachweise verlangt, sollten die Anforderungen an diese klar und verständlich formuliert sein sowie die Stelle benannt werden, gegenüber der die Legitimation erfolgen kann.
Für Details zu dieser Empfehlung siehe Kapitel 7.4 auf Seite 316 und 7.5 auf Seite 330.

U 9: Dienstanbietern ist darüber hinaus zu empfehlen, jegliche Koppelung zu vermeiden, die die (einfache und effektive) Durchsetzung eines digitalen Nachlasses an die Bedingung knüpft, dass es sich bei dem Erben ebenfalls um einen Nutzer des Dienstes handeln muss. Auch sind sonstige Benachteiligungen von Erben, die keine Dienstnutzer sind, im Vergleich zu Erben, die Dienstnutzer sind, zu vermeiden.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.4 auf Seite 167.

An sonstige Unternehmen und Institutionen können folgende Empfehlungen gerichtet werden:

UI 1: Unabhängigen Institutionen wie z. B. Verbraucherverbänden und der Stiftung Warentest kann empfohlen werden, die von Dienstanbietern an deren Nutzer bereitgestellten Informationen zum digitalen Nachlass sowie ggf. bestehende Unterstützungsleistungen der Dienstanbieter zur Planung und Durchsetzung eines digitalen Nachlasses zu vergleichen. Ggf. könnte sogar ein „Siegel zum digitalen Nachlass“ entwickelt werden.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.2 auf Seite 164.

UI 2: Da Erblassern derzeit häufig weder bewusst ist, was mit ihren persönlichen Daten und finanziellen, digitalen Werten nach ihrem Tod passieren wird, noch ihnen bewusst ist, dass sie darauf aktiv Einfluss nehmen können, ist zudem zu empfehlen, Verbraucher z. B. im Rahmen von Awarenesskampagnen auch in Zukunft für das Thema des digitalen Nachlasses zu sensibilisieren. Solche Kampagnen sollten insbesondere von Verbraucherschutzverbänden und/oder dem Gesetzgeber durchgeführt werden.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.7 auf Seite 169.

8.4 Empfehlungen für den Gesetzgeber und die Verwaltung

An den Gesetzgeber und die Verwaltung können folgende Empfehlungen gerichtet werden:

GV 1: Die Regelungen zum Zentralen Testamentsregister könnten um die Möglichkeit erweitert werden, auch die sog. digitale Vorsorgeurkunde zu registrieren. So wäre es möglich, das Verfahren zu zentralisieren und zu vereinfachen. Für die Verbraucher würde dies weitere Sicherheit bieten. Zudem wäre im Erbfall eine zügige Abwicklung möglich, da die Existenz der Vorsorgeurkunde im Rahmen der Testamentseröffnung bekannt gegeben werden könnte.
Für Details zu dieser Empfehlung siehe Kapitel 6.5.9.3 auf Seite 223.

GV 2: Im Beurkundungsgesetz könnte die Möglichkeit vorgesehen werden, dass Notare Ausfertigungen von Urkunden auch in elektronischer Form erteilen können. So könnte die Legitimation von Vorsorgebevollmächtigten im digitalen Rechtsverkehr vereinfacht werden. Hierbei sind aber technisch die Sicherheitsanforderungen an eine solche digitale Ausfertigung sicherzustellen, um weiter den Beweiswert der Ausfertigung gewährleisten zu können.
Für Details zu dieser Empfehlung siehe Kapitel 6.6.4.3 auf Seite 257.

GV 3: Alternativ zum vorhergehenden Vorschlag wäre es auch aus Sicht des digitalen Bereichs sinnvoll, das Elektronische Urkundenarchiv zu einem Vollmachts- und Titelregister weiterzuentwickeln. Auf diese Weise könnte die Legitimation von Vorsorgebevollmächtigten zukünftig digital erfolgen und so vereinfacht werden.
Für Details zu dieser Empfehlung siehe Kapitel 6.6.4.4 auf Seite 259.

GV 4: Der Schutzumfang, den die §§ 305 ff. BGB in Bezug auf die wirksame Einbeziehung und die Wirksamkeit von AGB für Verbraucher vorsehen, scheint vollständig. Änderungsbedarf an den §§ 305 ff. BGB ergibt sich daher nicht. Jedoch sollte die Diskussion um die Rechtsdurchsetzung von Ansprüchen der Verbraucher fortgesetzt werden.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.1 auf Seite 162.

GV 5: Darüber hinaus kann empfohlen werden, über eine repräsentative Umfrage zu klären, ob seitens der Verbraucher im Rahmen der Dienstnutzung (und in den zugehörigen Anbieter-AGB) die Notwendigkeit besteht, das Wort „Kaufen“ von dem „Erwerb einer lebenslangen Lizenz“ abzugrenzen, um den Verbrauchern aufzuzeigen, dass ein digitaler Wert, wie z. B. eine digitale Musikdatei, ggf. nach dessen Tod nicht vererbbar ist.[3]
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.3 auf Seite 166.

GV 6: Da Erblassern derzeit häufig weder bewusst ist, was mit ihren persönlichen Daten und finanziellen, digitalen Werten nach ihrem Tod passieren wird, noch ihnen bewusst ist, dass sie darauf aktiv Einfluss nehmen können, ist zudem zu empfehlen, Verbraucher z. B. im Rahmen von

[3] Ein genereller Ausschluss der Vererblichkeit eines *Nutzerkontos* in AGB wird in der Literatur überwiegend für unwirksam erachtet. Eine *Lizenz an digitalen Werten* – wie z. B. Musik- oder Filmdateien – kann demgegenüber i. d. R. in den AGB wirksam auf die Lebzeit des Erblassers beschränkt werden.

Awarenesskampagnen auch in Zukunft für das Thema des digitalen Nachlasses zu sensibilisieren.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.7 auf Seite 169.

GV 7: Eine Sensibilisierung der Verbraucher kann auch durch eine gesetzlich geregelte Informationsverpflichtung der Dienstanbieter erreicht werden. Empfohlen wird eine gesetzliche Informationspflicht für Dienstanbieter hinsichtlich einer Verarbeitung von personenbezogenen Daten nach dem Tod. Den Verbrauchern sollte auf diesem Wege transparent dargelegt werden, dass die zu Lebzeiten verarbeiteten personenbezogenen Daten mit dem Tod nicht einfach gelöscht oder auf sonstige Weise entfernt werden. Die gesetzliche Informationspflicht soll sich aus drei Elementen zusammensetzen: Dienstanbieter sollten im Rahmen ihrer AGBs mindestens (1) einen Hinweis auf den grundsätzlichen Übergang des Nutzerkontos und der darin enthaltenen Daten auf die Erben geben. (2) Weiterhin sollten die Dienstanbieter verpflichtet werden, dem Verbraucher als Nutzer des Online-Dienstes eine oder mehrere Wahlmöglichkeiten hinsichtlich der Regelung des Verfahrens mit den Daten nach dem Tod zur Verfügung zu stellen. Schließlich (3) bedarf es eines Hinweises auf die Möglichkeit, eine detailliertere und weitergehende Vorsorge im Rahmen einer letztwilligen Verfügung oder einer Bevollmächtigung auf den Tod zu treffen.
Für Details zu dieser Empfehlung siehe Kapitel 5.5.2.2 auf Seite 164.

9 Vorlagen

Mittlerweile existiert eine Vielzahl von Formulierungsvorschlägen und Mustern für Vorsorgevollmachten und letztwillige Verfügungen.

Zunächst ist darauf hinzuweisen, dass die nachfolgenden Vorlagen sich allein auf die digitalen Angelegenheiten bzw. den digitalen Nachlass beziehen und die Formulierungen sowohl in den Vorsorgevollmachen als auch den letztwilligen Verfügungen auf diesen Bereich beschränkt sind. Weitergehende Formulierungen werden nur aufgenommen, soweit dies für die Wirksamkeit der Urkunde erforderlich ist.

Auch ist darauf hinzuweisen, dass trotz der nachfolgenden Vorlagen – insbesondere aufgrund des vermutlich über den digitalen Bereich hinausgehenden Regelungsbedarfs – die Beratung durch einen Notar empfehlenswert ist. Zudem sollte insbesondere jede letztwillige Verfügung den Einzelfall berücksichtigten, da es sonst zu Problemen im Rechtsverkehr oder Streitigkeiten kommen kann. Hinsichtlich der ungeprüften Übernahme von Vorlagen ist daher Vorsicht geboten. Die Muster können jedoch als Orientierungshilfe dienen.

9.1 Vorsorgevollmacht

Eine Vollmacht allein für die digitalen Angelegenheiten kann folgendermaßen formuliert werden:

Vorsorgevollmacht für digitale Angelegenheiten

Ich, *< Name, Vorname des Vollmachtgebers >*,

< Geburtsdatum >,
< Geburtsort >,
< Adresse >,
< Telefon, Telefax, E-Mail >

Erteile hiermit Vollmacht an

< Name, Vorname des Bevollmächtigten >,
< Geburtsdatum >,
< Geburtsort >,

< Adresse >,
< Telefon, Telefax, E-Mail >

Diese Vertrauensperson wird hiermit bevollmächtigt, mich in allen Angelegenheiten zu vertreten, die ich im Folgenden angekreuzt oder angegeben habe. Durch diese Vollmachtserteilung soll eine vom Gericht angeordnete Betreuung vermieden werden. Die Vollmacht bleibt daher in Kraft, wenn ich nach ihrer Errichtung geschäftsunfähig geworden sein sollte.

1. Digitale Angelegenheiten

Die bevollmächtigte Person darf unabhängig vom Zugangsmedium meinen gesamten Datenbestand einschließlich der bei Dritten (Internetdienstanbietern) gespeicherten Daten und meine sämtlichen Vertragsbeziehungen betreffend informationstechnische Systeme verwalten. Zudem darf sie alle für diese Angelegenheiten erforderlichen Handlungen vornehmen sowie alle damit zusammenhängenden Willenserklärungen abgeben. Sie darf auch sämtliche hierzu erforderlichen Zugangsdaten nutzen und diese anfordern.

2. Post- und Fernmeldeverkehr

Sie darf im Rahmen der Ausübung dieser Vollmacht die für mich bestimmte elektronische Post entgegennehmen, öffnen und lesen. Zudem darf sie über den Fernmeldeverkehr einschließlich aller elektronischen Kommunikationsformen entscheiden.

3. Vertretung vor Gericht

Sie darf mich gegenüber Gerichten vertreten sowie Prozesshandlungen aller Art vornehmen.

4. Untervollmacht

Sie darf (keine) Untervollmacht erteilen.

5. Betreuungsverfügung

Falls trotz dieser Vollmacht eine gesetzliche Vertretung (rechtliche Betreuung) erforderlich sein sollte, bitte ich, die oben bezeichnete Vertrauensperson als Betreuer zu bestellen.

6. Geltung über den Tod hinaus

Die Vollmacht gilt über den Tod hinaus.

Ort, Datum, Unterschrift des/der Vollmachtnehmers/in

Ort, Datum, Unterschrift des/der Vollmachtgebers/in

Ein Muster für eine umfassende Vorsorgevollmacht findet sich auf den Internetseiten des BMJV.[1] Soll die Bevollmächtigung für die digitalen Angelegenheiten in eine Vollmacht eingebettet werden, kann nach dem Punkt zum Post- und Fernmeldeverkehr folgende Ergänzung erfolgen:

> **6. Digitale Angelegenheiten**
>
> Sie darf unabhängig vom Zugangsmedium meinen gesamten Datenbestand einschließlich der bei Dritten (Internetdienstanbietern) gespeicherten Daten und meine sämtlichen Vertragsbeziehungen betreffend informationstechnische Systeme verwalten. Zudem darf sie alle für diese Angelegenheiten erforderlichen Handlungen vornehmen sowie alle damit zusammenhängenden Willenserklärungen abgeben.
>
> Sie darf auch sämtliche hierzu erforderlichen Zugangsdaten nutzen und diese anfordern.

Erläuterungen:

Die Vollmacht ist möglichst weit gefasst. Legt der Vollmachtnehmer die Vollmacht einem Online-Dienstanbieter vor und loggt er sich bei dem Nutzerkonto ein, darf er sämtliche Handlungen vornehmen, zu denen auch der Vollmachtgeber befugt ist. Dazu gehört es beispielsweise, E-Mails zu lesen und zu beantworten. Der Vollmachtnehmer dürfte sogar Nutzerkonten löschen. Auch darf der Vollmachtnehmer alle auf Speichermedien des Vollmachtgebers (Computer, externe Festplatten, USB-Sticks etc.) befindlichen Daten ansehen.

Auf eine Aufzählung von einzelnen digitalen Angelegenheiten oder Berechtigungen wird verzichtet, da so die Gefahr besteht, die Vollmacht ungewollt zu beschränken. Für den Verbraucher können stets neue digitale Angelegenheiten hinzukommen, die nicht Teil einer Auflistung sind, weil sie zum Zeitpunkt der Vollmachtserteilung noch nicht relevant waren oder schlicht vergessen wurden. So kann jedoch im Rechtsverkehr der Eindruck entstehen, dass diese Angelegenheit nicht von der Bevollmächtigung umfasst ist. Dies kann selbst dann der Fall sein, wenn die Auflistung mit „insbesondere“ eingeleitet wird.

In Punkt 6 ist festgelegt, dass die Vollmacht über den Tod hinaus gilt. Somit könnte der Vollmachtgeber auch gegenüber den Erben tätig werden und auch nach dem Tod die Daten des verstorbenen Vollmachtgebers weiter verwalten. Ist dies nicht gewünscht, kann dieser Punkt gestrichen werden.

Möchte der Vollmachtgeber die Bevollmächtigung beschränken, und erreichen, dass sich der Vollmachtnehmer in einer bestimmten Weise verhält, kann dies dadurch erreicht werden, dass der Vollmachtgeber dem Vollmachtnehmer *auf einem anderen Blatt Papier oder in einem anderen Dokument* besondere Anweisungen erteilt. Sonst ist aber keine besondere Form für dieses Dokument einzuhalten. Dieses Dokument ist Geschäftspartnern nicht vorzulegen, sondern ist nur für Vollmachtgeber und

[1] BMJV, Formulare zur Vorsorgevollmacht, https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Formulare/Vorsorgevollmacht.html?nn=6765634.

Vollmachtnehmer bestimmt. Beide sollten ein Exemplar dieses Dokuments haben. Der Vollmachtgeber ist mit seinen Anweisungen sehr frei, solange er vom Vollmachtnehmer nichts verlangt, was verboten ist.
So kann beispielsweise bestimmt werden, dass der Vollmachtnehmer nur auf das Onlinebanking oder Online-Bezahldienst-Konten zugreifen darf, nicht aber auf Social-Media-Profile. Auch kann bestimmt werden, dass der Vollmachtnehmer in einer bestimmten Art und Weise handeln soll oder erst nach Eintritt der Handlungsunfähigkeit von der Vollmacht Gebrauch machen darf. Insbesondere letztere Anweisung empfiehlt sich, wenn der Vollmachtnehmer erst dann tätig werden soll, wenn sich der Vollmachtgeber aus gesundheitlichen Gründen (alters- oder krankheitsbedingt) nicht mehr selbst um seine Angelegenheiten kümmern kann.

Auch wenn der Vollmachtnehmer durch die Vollmacht ermächtigt wird, die Zugangsdaten anzufordern, ist zu empfehlen, die Zugangsdaten so für den Vollmachtnehmer sicher zu hinterlegen, dass dieser im Ernstfall Zugriff hierauf nehmen kann. So kann auch sichergestellt werden, dass der Vollmachtnehmer im Ernstfall von allen relevanten Nutzerkonten und Datenspeichern weiß.
Erneut ist allerdings darauf hinzuweisen, dass die Zugangsdaten auf keinen Fall direkt in die Vollmachtsurkunde aufgenommen werden sollten.
Entweder kann eine weitere gesonderte Liste auf Papier mit den Nutzernamen und Passwörtern angefertigt werden. Allerdings besteht hier die Gefahr, dass die Liste verloren geht oder Personen die Liste finden, die die Passwörter nicht erfahren sollen.
Daher kann die ausführlich in Kapitel 6.5.8 auf Seite 217 beschriebene Konstruktion der „digitalen Vorsorgeurkunde“ empfohlen werden. Hierbei sichert der Vollmachtgeber die stets aktuell zu haltenden Zugangsdaten auf einem verschlüsselten lokalen Datenträger (z. B. einem USB-Stick). Zur Speicherung der Zugangsdaten empfiehlt sich die Verwendung des Programms KeePass. Dieser Datenträger ist mit einem Masterpasswort gesichert, das bei einer Vertrauensperson, beispielsweise einem Notar, hinterlegt ist. Hat der Vollmachtgeber hiervon Gebrauch gemacht, kann zur Erleichterung des Zugangs des Vollmachtnehmers zu den digitalen Inhalten folgender Satz im Rahmen des gesonderten Dokuments mit den Anweisungen aufgenommen werden:

> Sämtliche erforderlichen Zugangsdaten für die digitalen Inhalte sind auf einem verschlüsselten lokalen Datenträger *<genauere Beschreibung>* gespeichert. Dieser befindet sich *<genauere Beschreibung des Aufbewahrungsortes>*. Das Masterpasswort hierzu habe ich zur Urkunde des Notars *<Name, Anschrift des Notariats>*, vom *<genaues Datum>*, UR-Nr. <...>, niederschreiben lassen.

Der letzte Satz dieser Formulierung gilt nur, wenn das Masterpasswort tatsächlich von einem Notar aufbewahrt wird. Bewahrt eine andere Person das Masterpasswort auf, sind deren Kontaktdaten zu vermerken. Daneben ist auch denkbar, dass der Vollmachtgeber dem Vollmachtnehmer die Liste der Zugangsdaten sogleich mit der Vollmachtserteilung aushändigt. Allerdings sollte in diesem Fall ein großes Vertrauen des Vollmachtgebers in den Vollmachtnehmer bestehen, dass dieser nicht vorzeitig Zugriff auf die Daten nimmt.

Speziell zur Erweiterung des Vollmachtsmusters des BMJV:

Durch diese Erweiterung der Vollmacht wird die Ermächtigung zu allen für die digitalen Angelegenheiten erforderlichen Handlungen und Willenserklärungen umfasst. Die besondere Vollmacht für den Fernmeldeverkehr ist schon in Punkt 5 des Musters des BMJV angeführt und daher hier nicht mehr gesondert erforderlich.

9.2 Letztwillige Verfügungen

Möglich ist es aber auch, durch ein Testament zu bestimmen, was nach dem Tod mit den eigenen Daten geschehen soll.

Ein Testament ist unbedingt per Hand zu verfassen, da es sonst aufgrund eines Formfehlers nicht wirksam ist. Soweit die vorgeschlagenen Textbausteine übernommen werden, müssen diese somit *zwingend mit der Hand abgeschrieben* werden.

9.2.1 Erbeinsetzung hinsichtlich des digitalen Nachlasses

Grundsätzlich gilt, dass der digitale Nachlass im Wege der Gesamtrechtsnachfolge i. S. d. § 1922 BGB auf die Erben übergeht. Es ist daher nicht unbedingt erforderlich, dass der Verbraucher (im Folgenden Erblasser) seinen digitalen Nachlass im Testament gesondert erwähnt. Sollen nur ein oder mehrere Erben eingesetzt werden, die das gesamte Vermögen des Erblassers erhalten sollen, reicht es, wenn nur die Erben benannt werden.

Formulierungsbeispiel:

Soll lediglich ein Alleinerbe oder mehrere Personen gleichberechtigt eingesetzt werden, reicht somit der einfache Satz:

Testament

Ich *< vollständiger Name >*, geboren am *< Geburtsdatum >*, setze hiermit *< vollständiger Name >*, geboren am *< Geburtsdatum >*, derzeit wohnhaft *< vollständige Adresse >*, als alleinigen Vollerben ein.

< Ort, Datum >

< Eigenhändige Unterschrift des Erblassers mit Vor- und Familiennamen >

Anmerkung:

Hinsichtlich der Anzahl der Erben ist der Erblasser frei. Sollen mehrere Personen gemeinsam und gleichberechtigt Erben werden, sind die Namen der Erben mit Geburtsdatum und derzeitiger Adresse einzufügen und die Formulierung „als alleinigen Vollerben“ durch „als alleinige gemeinsame Vollerben“ zu ersetzen.

Wenn dies gewünscht ist, kann lediglich *klarstellend* im Testament festgehalten werden, dass sich die Erbenstellung auch auf den digitalen Nachlass bezieht. Derartige Zusätze sind grundsätzlich möglich, allerdings sollte unbedingt zum Ausdruck kommen, dass es sich um eine rein deklaratorische Erläuterung handelt, um die Rechtsdurchsetzung sicherzustellen.[2] Auch droht hier die Gefahr, dass der Zusatz unpräzise oder lückenhaft formuliert ist und die Rechte der Erben unnötig beschränkt werden oder Auseinandersetzungen mit Dienstanbietern auftreten. Empfohlen wird daher – für den Fall, dass keine besonderen Anordnungen gewünscht sind – die erstgenannte Formulierung.

Eine klarstellende Formulierung könnte allerdings lauten:

Testament

Ich *< vollständiger Name des Erblassers >*, geboren am *< Geburtsdatum >*, setze hiermit *< vollständiger Name des Erben >*, geboren am *< Geburtsdatum >*, derzeit wohnhaft *< vollständige Adresse >*, als alleinigen Vollerben ein. Dabei stelle ich ausdrücklich klar, dass meine Erben gemäß § 1922 BGB gänzlich in meine Rechtsstellung, insbesondere auch in alle meine bestehenden Vertragsverhältnisse zu Internetdienstanbietern, eintreten sowie Anspruch auf alle meine lokal sowie auf fremden Servern gespeicherten geschäftlichen sowie privaten Daten haben.

< Ort, Datum >

< eigenhändige Unterschrift mit Vor- und Familiennamen >

Weitere Anmerkung:

Soweit von einer digitalen Vorsorgeurkunde Gebrauch gemacht wurde (siehe oben in Kapitel 6.5.8 auf Seite 217), kann nachfolgender Hinweis für die Erben angefügt werden, um es den Erben zu erleichtern, alle Nutzerkonten des Erblassers aufzufinden und auch tatsächlich auf diese zugreifen zu können. Erneut ist der letzte Satz des Formulierungsvorschlags darauf bezogen, dass das Masterpasswort tatsächlich bei einem Notar hinterlegt ist. Ist das Masterpasswort bei einer anderen Vertrauensperson hinterlegt, sind deren Kontaktdaten zu nennen:

[2] Insgesamt hierzu auch *Herzog/Pruns*, § 10 D Rn. 25 ff.

Sämtliche erforderlichen Zugangsdaten für die digitalen Inhalte sind auf einem verschlüsselten lokalen Datenträger <*genauere Beschreibung*> gespeichert. Dieser befindet sich <*genauere Beschreibung des Aufbewahrungsortes*>. Das Masterpasswort hierzu habe ich zur Urkunde des Notars <*Name, Anschrift des Notariats*>, vom <*genaues Datum*>, UR-Nr. <...>, niederschreiben lassen.

9.2.2 Vermächtnisse und Teilungsanordnungen

Sollen bestimmte digitale Inhalte einer bestimmten Person zugewendet werden, ist dies grundsätzlich durch die Anordnung eines Vermächtnisses oder einer Teilungsanordnung möglich. Eine solche Anordnung sollte in ein Testament eingebettet werden. Grundsätzlich gilt, dass allein durch eine Einsetzung als Erbe keine einzelnen Vermögensgegenstände auf eine bestimmte Person übertragen werden können. Allerdings kann der Erblasser dies dadurch steuern, indem er ein Vermächtnis oder eine Teilungsanordnung in seinem Testament vorsieht.

Vermächtnis bedeutet dabei grundsätzlich, dass einer Person ein Vermögensgegenstand zugewendet wird, ohne, dass diese Person auch Erbe wird. Die begünstigte Person (genannt Vermächtnisnehmer) hat aber einen Anspruch gegen die Erben, dass ihr der zugewendete Vermögensgegenstand herausgegeben wird.

Bei einer Teilungsanordnung wird bestimmt, wie die Erben bestimmte Gegenstände unter sich aufzuteilen haben. Ohne besondere Anordnungen gilt, dass die Erben den Nachlass nur gerecht unter sich aufzuteilen haben. Durch eine Teilungsanordnung kann der Erblasser aber erreichen, dass ein bestimmter Erbe einen bestimmten Gegenstand erhält, wenn dies gewünscht ist.

Da hier im Einzelfall die verschiedensten Anordnungen möglich sind, können nachfolgend nur einige Formulierungsbeispiele erfolgen. Hinsichtlich der weiteren rechtlichen Wirkungen sowie der Vor- und Nachteile der verschiedenen Anordnungsmöglichkeiten wird auf die Erläuterungen in Kapitel 6.4 auf Seite 181 verwiesen. Von diesen Formulierungsvorschlägen können, je nach Regelungswillen des Erblassers, Abweichungen bzw. Anpassungen vorgenommen werden.

Formulierungsbeispiele für ein Vermächtnis

Vermächtnis

Ich beschwere meine Erben mit folgendem Vermächtnis:

<*Name*>, geboren am <*Geburtsdatum*>, derzeit wohnhaft <*vollständige Adresse*>, erhält im Wege des Vermächtnisses den verschlüsselten lokalen Datenträger <*genaue Beschreibung des Datenträgers*> zu Alleineigentum mit sämtlichen darauf gespeicher-

ten Daten. Der Datenträger befindet sich *<genaue Beschreibung des Aufbewahrungsortes>*.

oder:

Vermächtnis

Ich beschwere meine Erben mit folgendem Vermächtnis:

<Name>, geboren am *<Geburtsdatum>*, derzeit wohnhaft *<vollständige Adresse>*, soll im Wege des Vermächtnisses in mein Vertragsverhältnis mit dem Internetdienstanbieter *<Firmenname und Sitz des Internetdienstanbieters>* eintreten.

Anmerkung:

Ist das Passwort für den digitalen Datenträger oder das vermachte Online-Vertragsverhältnis in einer digitalen Vorsorgeurkunde gespeichert, kann auf obiges Formulierungsbeispiel hierzu verwiesen werden.

Die beschriebenen Vermächtnisse können mit einer Auflage der Erben verbunden werden, keine Einsicht in die Vermächtnisgegenstände zu nehmen. Diese Auflage kann wiederum durch eine Testamentsvollstreckung abgesichert werden.

Formulierungsbeispiel Teilungsanordnung

Testament

Ich *<vollständiger Name>*, geboren am *<Geburtsdatum>*, setze hiermit *<vollständiger Name>*, geboren am *<Geburtsdatum>*, derzeit wohnhaft *<vollständige Adresse>* und *<vollständiger Name>*, geboren am *<Geburtsdatum>*, derzeit wohnhaft *<vollständige Adresse>* als meine alleinigen gemeinsamen Vollerben ein.

Im Rahmen der Auseinandersetzung des Nachlasses soll mein Erbe *<Name des Erben>*, den verschlüsselten Datenträger *<genaue Beschreibung des Datenträgers>* zu Alleineigentum mit sämtlichen darauf gespeicherten Daten erhalten. Dieser befindet sich *<genaue Beschreibung des Aufbewahrungsortes>*.

Mein Erbe *<Name des anderen Erben>* soll während des Bestehens der Erbengemeinschaft keine Einsicht auf den Datenträger nehmen.

Anmerkung:

In diesem Formulierungsbeispiel werden zwei Erben eingesetzt. Der Erblasser ist aber frei zu wählen, wie viele Erben er einsetzen möchte. Zu beachten ist allerdings, dass eine Teilungsanordnung nur erforderlich ist, wenn mehr als ein Alleinerbe eingesetzt wird. Im Beispiel soll ein Erbe allein auf einen lokalen Datenträger zugreifen können. Denkbar ist aber beispielsweise auch, dass ein Erbe nur auf ein bestimmtes Nutzerkonto oder eine Cloud zugreifen können soll.

9.2.3 Auflagen

Sollen sich die Erben hinsichtlich des digitalen Nachlasses auf eine bestimmte Weise verhalten, kann eine Beschwerung mit Auflagen erfolgen. Da hier im Einzelfall die verschiedensten Anordnungen möglich sind, können nachfolgend nur einige Beispiele erfolgen.

Hinsichtlich der Vor- und Nachteile der verschiedenen Anordnungsmöglichkeiten wird auf Kapitel 6.4 auf Seite 181 verwiesen.

Formulierungsbeispiele

Soll einem Begünstigten im Wege eines Vermächtnisses ein digitaler Inhalt übertragen werden und die Erben auf diesen keinen Zugriff nehmen, könnte eine entsprechende Auflage folgendermaßen lauten:

> Meine Erben beschwere ich mit der Auflage, dem Vermächtnisnehmer *<näher zu bezeichnender digitaler Inhalt, z. B. Cloud-Server-Zugang, Social-Media-Account, lokaler Datenträger etc.>* zu übertragen, ohne vorher Einsicht zu nehmen.

Sollen die Erben verpflichtet werden, bestimmte digitale Inhalte zu löschen, könnte folgende Anordnung erfolgen:

> Meine Erben beschwere ich mit der Auflage, mein Vertragsverhältnis mit dem Internetdienstanbieter *<Name des Internetdienstanbieters, Sitz>* nach meinem Ableben unverzüglich zu kündigen. Ihnen steht es frei, die darin gespeicherten Inhalte vorher lokal abzuspeichern.

oder:

> Meine Erben beschwere ich mit der Auflage, mein Vertragsverhältnis mit dem Inter-

> netdienstanbieter <*Name des Internetdienstanbieters, Sitz*> nach meinem Ableben unverzüglich zu kündigen, ohne vorher Einsicht zu nehmen.

Sollen die Erben einen bestimmten digitalen Inhalt in einer bestimmten Weise weiterführen:

> Auf meiner privaten Homepage <*Beschreibung der Homepage*> soll ein Hinweis zu meinem Ableben erscheinen. Die Kommentarfunktion soll gesperrt werden. Meinen Erben steht es frei, die darin gespeicherten Inhalte lokal abzuspeichern. Sechs Monate nach meinem Versterben sollen die Homepage und sämtliche Inhalte vollständig gelöscht werden.

9.2.4 Testamentsvollstreckung

Der Erblasser kann auch einen Testamentsvollstrecker einsetzen. Dieser hat dann die Aufgabe, den Nachlass so lange zu verwalten, bis er unter den Erben aufgeteilt ist. Die Testamentsvollstreckung ist eine gute Möglichkeit, um sicherzustellen, dass die Erben die testamentarischen Anordnungen des Erblassers auch befolgen. Die Erben sind bei Anordnung einer Testamentsvollstreckung gewissen Beschränkungen hinsichtlich des Nachlasses unterworfen und können nicht frei über diesen verfügen. Auch dem Testamentsvollstrecker können Anordnungen dahingehend gegeben werden, welche Teile des Nachlasses er verwalten oder wie er sich im Hinblick auf einzelne Nachlassgegenstände verhalten soll.

Soll ein Testamentsvollstrecker für den digitalen Nachlass eingesetzt werden, ist zu empfehlen, eine Person auszuwählen, die das notwendige technische Verständnis und Wissen mitbringt.

Auch hinsichtlich der Testamentsvollstreckung ist die Formulierung daran auszurichten, welche Befugnisse der Testamentsvollstrecker wahrnehmen soll. Da hier im Einzelfall die verschiedensten Anordnungen möglich sind, können nachfolgend nur einige Beispiele erfolgen. Hinsichtlich der Vor- und Nachteile der verschiedenen Anordnungsmöglichkeiten wird auf Kapitel 6.4 auf Seite 181 verwiesen.

Formulierungsbeispiele

Soll allgemein Testamentsvollstreckung ohne Einschränkung der Befugnisse des Testamentsvollstreckers angeordnet werden, reicht folgende Formulierung:

> Ich ernenne <*vollständiger Name, Geburtsdatum, vollständige Adresse*> zu meinem Testamentsvollstrecker mit der Aufgabe und Befugnis, meinen Nachlass zu verwalten und auseinanderzusetzen.
>
> Will oder kann der vorgesehene Testamentsvollstrecker das Amt nicht antreten oder

> fällt er vor seiner Ausführung weg, soll *<vollständiger Name, Geburtsdatum, derzeitige Adresse>* die Aufgaben und Befugnisse des Testamentsvollstreckers wahrnehmen.

Soll der Testamentsvollstrecker eine Vergütung erhalten, kann ein entsprechender Satz angefügt werden:

> Der Testamentsvollstrecker erhält für seine Tätigkeit eine angemessene Vergütung. Diese richtet sich nach den bei Errichtung dieser Verfügung von Todes wegen aktuellen Vergütungsempfehlungen des Deutschen Notarvereins.

Für den Fall, dass der Testamentsvollstrecker keine Vergütung erhalten soll, kann diese auch ausgeschlossen werden.

Soll der Testamentsvollstrecker nur den digitalen Nachlass regeln, die Erben vom Zugriff auf diesen ausschließen und gemäß der Auflagen und Vermächtnisse des Erblassers unter diesen verteilen, kann folgende Formulierung erfolgen (im vorliegenden Beispiel liegt eine digitale Vorsorgeurkunde vor):

> Es ist Aufgabe des Testamentsvollstreckers, unter Ausschluss der Erben meine Zugangsdaten zu sämtlichen digitalen Inhalten an sich zu nehmen. Sämtliche erforderlichen Zugangsdaten für die digitalen Inhalte sind auf einem verschlüsselten lokalen Datenträger *<genauere Beschreibung>* gespeichert. Dieser befindet sich *<genauere Beschreibung des Aufbewahrungsorts>*. Das Masterpasswort hierzu habe ich zur Urkunde des Notars *<Name, Anschrift des Notariats>*, vom *<genaues Datum>*, UR-Nr. *<...>*, niederschreiben lassen.
>
> Es ist weitere Aufgabe und Befugnis des Testamentsvollstreckers, die von mir ausgesetzten Vermächtnisse und Auflagen hinsichtlich der digitalen Inhalte zu erfüllen und zu überwachen.
>
> Insbesondere soll er: *<besondere Anordnungen>*

9.3 Optionsrecht des Verbrauchers als vertragliche Regelung

9.3.1 Optionsrecht für den Todesfall

Das Vertragsverhältnis geht im Fall Ihres Todes auf Ihre Erben über.
Das bedeutet, dass die Erben Zugriff auf Ihr Nutzerkonto und die dort gespeicherten Inhalte nehmen können, wenn Sie keine anderweitige Regelung (z. B. durch letztwillige Verfügung oder Vollmacht) treffen.

Sie können aber auch an dieser Stelle gegenüber dem Vertragspartner bestimmen, was nach Ihrem Tod mit dem Vertragsverhältnis geschehen soll.

Im Fall meines Todes wünsche ich,

☐ dass mein Konto und alle meine Daten vollständig und unwiederbringlich gelöscht werden.
Mir ist bewusst, dass nach der Löschung niemand mehr auf meine Daten zugreifen kann. Dazu gehören unter anderem die von mir geschriebenen Nachrichten, meine geteilten Inhalte und meine Kontakte. Das Konto wird gelöscht, wenn *< vollständiger Name, E-Mail-Adresse >* durch Vorlage der Kopie oder eines Scans meiner Sterbeurkunde meinen Tod beweist. Die Mitteilung ist an folgende Adresse zu senden: *< Anschrift oder E-Mail-Adresse der zuständigen Stelle >*
Erfolgt keine Mitteilung durch die benannte Person, wird mein Konto auch dann gelöscht, wenn meine Erben mir gegenüber den Todesfall anzeigen. Meinen Erben wird auch dann kein Zugriff auf mein Konto gewährt, wenn sie nachweisen, dass sie Erben sind.
Melden sich auch meine Erben nicht, wird mein Konto gelöscht, wenn ich es über einen Zeitraum von einem Jahr nicht benutzt habe.
In jedem Fall werde ich mindestens 21 Tage vor der Löschung durch eine Mitteilung an folgende E-Mail-Adresse *< E-Mail-Adresse >* gewarnt. Melde ich mich daraufhin erneut bei meinem Konto an, werden die Daten nicht gelöscht;

☐ dass mein Konto in den Gedenkzustand versetzt wird und von *< vollständiger Name, E-Mail-Adresse >* verwaltet wird. Diese Person hat die Befugnis, die Gedenkbeiträge in meinem Profil zu verwalten, die Löschung meines Kontos zu beantragen, auf neue Freundschaftsanfragen zu antworten und mein Profil- und Titelbild zu aktualisieren. Die benannte Person kann ausschließlich Beiträge verwalten, die nach meinem Tod erstellt wurden. Sie kann weder Beiträge in meinem Namen veröffentlichen noch meine Nachrichten einsehen.
Das Konto wird in den Gedenkzustand versetzt, wenn *< vollständiger Name, E-Mail-Adresse >* durch Vorlage der Kopie oder eines Scans meiner Sterbeurkunde meinen Tod beweist. Die Mitteilung ist an folgende Adresse zu senden: *< Anschrift oder E-Mail-Adresse der zuständigen Stelle >*;

☐ dass *< vollständiger Name, E-Mail-Adresse >* mein Konto einsehen, meine Daten speichern und das Konto anschließend löschen kann. Diese Person soll nicht befugt sein, Nachrichten von meinem Konto zu senden, Inhalte zu teilen oder das

Konto sonst in irgendeiner Art über die bloße Einsichtnahme hinaus zu nutzen. Dies ist mir bewusst.
Die genannte Person muss meinen Tod durch Vorlage der Kopie oder eines Scans meiner Sterbeurkunde beweisen. Das Dokument ist an folgende Adresse zu senden: *< Anschrift oder E-Mail-Adresse der zuständigen Stelle >*
Anschließend erhält sie meine Zugangsdaten vom Vertragspartner;

☐ dass *< vollständiger Name, E-Mail-Adresse >* mit allen Rechten und Pflichten als mein Nachfolger in das Vertragsverhältnis eintritt. Diese Person ist befugt, mein Konto in derselben Weise wie ich zu nutzen. Dazu gehört unter anderem, dass sie alle Inhalte einsehen, Nachrichten versenden, Inhalte teilen und das Konto löschen darf. Dies ist mir bewusst.
Die genannte Person muss meinen Tod durch Vorlage der Kopie oder eines Scans meiner Sterbeurkunde beweisen. Das Dokument ist an folgende Adresse zu senden: *< Anschrift oder E-Mail-Adresse der zuständigen Stelle >*
Anschließend erhält sie meine Zugangsdaten vom Vertragspartner.

☐ Ich wünsche keine Regelung für meinen Todesfall zu treffen.
Ich bin mir bewusst, dass meine Erben in diesem Fall nachweisen müssen, dass sie Erben sind.

☐ Ich möchte mich zu diesem Zeitpunkt noch nicht festlegen.
Ich bin mir bewusst, dass im Fall meines Todes meine Erben nachweisen müssen, dass sie Erben sind.

Mir ist bewusst, dass meine jetzt getroffene Auswahl nicht endgültig ist und dass ich meine Meinung jederzeit durch Anpassung der hier getroffenen Einstellungen ändern kann.

Die benannten Personen werden über die angegebene E-Mail-Adresse benachrichtigt und ihnen darin erklärt, was die Entscheidung für sie bedeutet.

Anmerkung:

Der vorliegende Formulierungsvorschlag ist an den Erfordernissen eines Social-Media-Accounts ausgerichtet. Handelt es sich um ein Online-Vertragsverhältnis mit einem anderen Inhalt, sind insbesondere gegebenenfalls die Regelungen zum Gedenkzustand obsolet und die Handlungsbefugnisse der Erben an die Bedürfnisse des jeweiligen Vertrages anzupassen. Ist eine Regelung mit weniger Alternativen für den Verbraucher gewünscht, ist zu beachten, dass jedenfalls die Möglichkeiten der Löschung, der Weitergabe und des Verzichts auf eine Regelung erforderlich sind. Gegebenenfalls können bei den einzelnen Regelungsalternativen auch Überschriften eingefügt werden, die knapp die Regelung umschreiben. Dadurch wird die Erläuterung der Regelung aber nicht überflüssig, diese ist für das Verständnis des Verbrauchers erforderlich.

9.3.2 Optionsrecht für den Fall der Handlungsunfähigkeit

Für den Fall, dass ich aus gesundheitlichen Gründen nicht mehr selbst in der Lage bin, mich um meine Angelegenheiten zu kümmern (Handlungsunfähigkeit), wünsche ich,

☐ dass mein Konto und alle meine Daten vollständig und unwiederbringlich gelöscht werden.
Mir ist bewusst, dass nach der Löschung niemand mehr auf meine Daten zugreifen kann. Dazu gehören unter anderem die von mir geschriebenen Nachrichten, meine geteilten Inhalte und meine Kontakte.
Das Konto wird gelöscht, wenn *<vollständiger Name, E-Mail-Adresse>* die Kopie oder einen Scan eines ärztlichen Attests vorlegt. Das ärztliche Attest muss folgende Voraussetzungen erfüllen: *<genauere Benennung der Voraussetzungen>*
Die Mitteilung ist an folgende Adresse zu senden: *<Anschrift oder E-Mail-Adresse der zuständigen Stelle>*.
Mein Konto wird auch gelöscht, wenn ich dies hier bestimmt habe und eine dem Vertragspartner unbekannte Person eine Vorsorgevollmacht vorlegt mit dem Begehren, Zugriff auf das Konto zu erhalten. Dem Bevollmächtigten wird auch dann kein Zugriff auf mein Konto gewährt, wenn er seine Vollmacht beweist.
Erfolgt keine Mitteilung durch die benannte Person, wird mein Konto gelöscht, wenn ich es über einen Zeitraum von einem Jahr nicht benutzt habe.
In jedem Fall werde ich mindestens 21 Tage vor der Löschung durch eine Mitteilung an folgende E-Mail-Adresse *< E-Mail-Adresse >* gewarnt. Melde ich mich daraufhin erneut bei meinem Konto an, werden die Daten nicht gelöscht;

☐ dass *< vollständiger Name, E-Mail-Adresse >* als mein Stellvertreter tätig wird. Die benannte Person darf mein Konto einsehen, meine Daten speichern und das Konto anschließend löschen. Sie soll nicht befugt sein, Nachrichten von meinem Konto zu senden, Inhalte zu teilen oder das Konto sonst in irgendeiner Art über die bloße Einsichtnahme hinaus zu nutzen.
Die genannte Person muss ihre Berechtigung gegenüber dem Vertragspartner nicht mehr gesondert nachweisen. Ich bin jedoch selbst dafür verantwortlich, der benannten Person meine Zugangsdaten mitzuteilen. Mir ist bewusst, dass ich das Risiko dafür trage, dass sich die benannte Person gemäß meinen Anweisungen verhält.
Ich erhalte aber eine Mitteilung an folgende E-Mail-Adresse *< E-Mail-Adresse >*, wenn sich eine Person neu bei meinem Konto anmeldet. Ich habe dann Gelegenheit, der Anmeldung durch Befolgung der Anweisungen in der mir zugesendeten E-Mail zu widersprechen. Reagiere ich nicht auf die E-Mail, darf der Vertragspartner vermuten, dass ich mit der Anmeldung einverstanden bin.
Auch wenn die Person die Anweisung zur Löschung des Kontos erteilt, werde ich durch Mitteilung an die angegebene E-Mail-Adresse gewarnt. Ich habe dann 21 Ta-

ge Zeit, mich erneut bei meinem Konto anzumelden. Erfolgt keine neue Anmeldung bei meinem Konto, werden die Daten gelöscht;

☐ dass *<vollständiger Name, E-Mail-Adresse)* als mein Stellvertreter tätig wird. Die benannte Person darf mein Konto verwalten und alle Handlungen vornehmen, zu denen auch ich befugt bin. Dazu gehört unter anderem, dass sie alle Inhalte einsehen, Nachrichten versenden, Inhalte teilen und das Konto löschen darf.
Die genannte Person muss ihre Berechtigung gegenüber dem Vertragspartner nicht mehr gesondert nachweisen. Ich bin jedoch selbst dafür verantwortlich, der benannten Person meine Zugangsdaten mitzuteilen. Mir ist bewusst, dass ich das Risiko dafür trage, dass sich die benannte Person gemäß meinen Anweisungen verhält.
Ich erhalte aber eine Mitteilung an folgende E-Mail-Adresse *<E-Mail-Adresse>*, wenn sich eine Person neu bei meinem Konto anmeldet. Ich habe dann Gelegenheit, der Anmeldung durch Befolgung der Anweisungen in der mir zugesendeten E-Mail zu widersprechen. Reagiere ich nicht auf die E-Mail, darf der Vertragspartner vermuten, dass ich mit der Anmeldung einverstanden bin.
Auch wenn die Person die Anweisung zur Löschung des Kontos erteilt, werde ich durch Mitteilung an die angegebene E-Mail-Adresse gewarnt. Ich habe dann 21 Tage Zeit, mich erneut bei meinem Konto anzumelden. Erfolgt keine neue Anmeldung bei meinem Konto, werden die Daten gelöscht;

☐ Ich wünsche keine Regelung für den Fall zu treffen, dass ich mich aus gesundheitlichen Gründen nicht mehr um meine Angelegenheiten kümmern kann (Handlungsunfähigkeit).
Mir ist bewusst, dass in diesem Fall die Möglichkeit besteht, dass von mir vorgenommene Handlungen durch den Vertragspartner nicht mehr anerkannt werden, wenn dieser den begründeten Verdacht hat, dass ich nicht mehr handlungsfähig bin.
Habe ich einer Person eine Vorsorgevollmacht erteilt und sie nicht gegenüber dem Vertragspartner benannt, ist diese Person befugt, alle Handlungen gegenüber dem Dienstanbieter für mich vorzunehmen, für die sie durch die Vollmacht ermächtigt ist, wenn die Person ihre Bevollmächtigung gegenüber dem Vertragspartner nachweist. Entsprechendes gilt, wenn gerichtlich ein Betreuer bestellt wurde.

☐ Ich möchte mich derzeit noch nicht festlegen.
Mir ist bewusst, dass in diesem Fall die Möglichkeit besteht, dass von mir vorgenommene Handlungen durch den Vertragspartner nicht mehr anerkannt werden, wenn dieser den begründeten Verdacht hat, dass ich nicht mehr handlungsfähig bin.
Habe ich einer Person eine Vorsorgevollmacht erteilt und sie nicht gegenüber dem Vertragspartner benannt, ist diese Person befugt, alle Handlungen gegenüber dem Dienstanbieter für mich vorzunehmen, für die sie durch die Vollmacht ermächtigt ist, wenn die Person ihre Bevollmächtigung gegenüber dem Vertragspartner nachweist. Entsprechendes gilt, wenn gerichtlich ein Betreuer bestellt wurde.

> Mir ist bewusst, dass meine jetzt getroffene Auswahl nicht endgültig ist und dass ich meine Meinung jederzeit durch Anpassung der hier getroffenen Einstellungen ändern kann.
>
> Die benannten Personen werden über die angegebene E-Mail-Adresse benachrichtigt und ihnen darin erklärt, was die Entscheidung für sie bedeutet. Habe ich selbst keine Vereinbarung mit dem Stellvertreter getroffen, ist mir bewusst, dass dieser das Recht hat, die Aufgabe zurückzuweisen.

Anmerkung:

Der vorliegende Formulierungsvorschlag ist an den Erfordernissen eines Social-Media-Accounts ausgerichtet. Handelt es sich um ein Online-Vertragsverhältnis mit einem anderen Inhalt, sind insbesondere gegebenenfalls die Regelungen zu den Handlungsbefugnissen des Stellvertreters an die Bedürfnisse des jeweiligen Vertrages anzupassen. Grundsätzlich kann auch eine Regelung mit weniger Alternativen für den Verbraucher getroffen werden. Ist aber die Benennung eines Stellvertreters vorgesehen, ist für die Wirksamkeit der vertraglichen Regelung zwingend, auch die Möglichkeit zu eröffnen, keine Regelung zu treffen und festzuhalten, dass ein Stellvertreter auch auf andere Weise bestellt sowie gegenüber dem Dienstanbieter tätig werden kann. Gegebenenfalls können bei den einzelnen Regelungsalternativen auch Überschriften eingefügt werden, die knapp die Regelung umschreiben. Dadurch wird die Erläuterung der Regelung aber nicht überflüssig, diese ist für das Verständnis des Verbrauchers erforderlich.

Über die beteiligten Forschungseinrichtungen

Fraunhofer SIT (Konsortialführer) Das Fraunhofer-Institut für Sichere Informationstechnologie SIT zählt zu den weltweit führenden Forschungseinrichtungen für Cybersicherheit und Privatsphärenschutz. Das Institut beschäftigt sich mit den zentralen Sicherheits- und Datenschutzherausforderungen in Wirtschaft, Verwaltung und Gesellschaft und betreibt praxisorientierte, interdisziplinäre Spitzenforschung zu allen Fragen der IT-Sicherheit und des IT-Rechts. Fraunhofer SIT ist Teil des Nationalen Forschungszentrums für angewandte Cybersicherheit (ATHENE), der europaweit größten Allianz von Forschungseinrichtungen im Bereich Cybersicherheit.

Kontakt: Michael Herfert, Leiter der Forschungsabteilung Cloud Computing, Identity & Privacy, Telefon: 06151-869-329, E-Mail: michael.herfert@sit.fraunhofer.de
Weitere Informationen finden Sie unter: www.sit.fraunhofer.de

Universität Bremen, IGMR (Konsortialpartner) Das Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) ist eine wissenschaftliche Einrichtung der Universität Bremen. Zentrale Zielsetzung des Instituts ist die interdisziplinäre Entwicklung von Lösungsansätzen für die Herausforderungen einer modernen Informationsgesellschaft. Prof. Dr. Benedikt Buchner lehrt an der Universität Bremen Bürgerliches Recht und Informationsrecht und ist geschäftsführender Direktor des IGMR. Er ist Mitherausgeber eines der führenden Kommentare zur Datenschutz-Grundverordnung und zum neuen BDSG sowie Mitherausgeber der Fachzeitschrift Datenschutz und Datensicherheit (DuD).

Kontakt: Prof. Dr. Benedikt Buchner, Direktor des Instituts für Informations-, Gesundheits- und Medizinrecht, Telefon: 0421 218-66044, E-Mail: bbuchner@uni-bremen.de
Weitere Informationen finden Sie unter: www.uni-bremen.de/jura/igmr

Universität Regensburg (Konsortialpartner) Die juristische Fakultät der Universität Regensburg ist eine der führenden deutschen Fakultäten im Bereich des Familien- und Erbrechts; zugleich ist sie europaweit hervorragend vernetzt. Die maßgeblichen Fachzeitschriften werden von Fakultätsmitgliedern verantwortet und zahlreiche Standardwerke von Fakultätsmitgliedern herausgegeben. Hinzu kommt eine weitreichende Beratungstätigkeit für das BMJV bei der Erarbeitung von Reformgesetzen.

Kontakt: Prof. Dr. Martin Löhnig, Lehrstuhl für Bürgerliches Recht, Rechtsgeschichte und Kirchenrecht, Telefon: 0941 943-2624, E-Mail: martin.loehnig@jura.uni-regensburg.de
Weitere Informationen finden Sie unter: https://www.uni-regensburg.de/rechtswissenschaft/buergerliches-recht/loehnig

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

a. A.	andere Ansicht, andere Auffassung
Abs.	Absatz
ACM	Association for Computing Machinery
AcP	Archiv für die civilistische Praxis (Zeitschrift)
a. E.	am Ende
AES	Advanced Encryption Standard (Algorithmus)
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
API	Application Programming Interface
Art.	Artikel
ASCII	American Standard Code for Information Interchange
BDSG	Bundesdatenschutzgesetz
BeckOGK	beck-online.GROSSKOMMENTAR
BeurkG	Beurkundungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BLE	Bundesanstalt für Landwirtschaft und Ernährung
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BNotO	Bundesnotarordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BtPtax	Betreuungsrechtliche Praxis (Zeitschrift)

BvD Berufsverband der Datenschutzbeauftragten Deutschlands (Zeitschrift: BvD-News)

BVerfG Bundesverfassungsgericht

CA Kanada (Länderkürzel)

CEF Connecting Europe Facility

CEN Comité Européen de Normalisation

CH Schweiz (Länderkürzel)

CHI ACM Conference on Human Factors in Computing Systems (Konferenz)

CIEC Commission Internationale de l'État Civil

CR Computer und Recht (Zeitschrift)

CSCW ACM Conference on Computer-Supported Cooperative Work and Social Computing

c't magazin für computertechnik (Zeitschrift)

DE Deutschland (Länderkürzel)

DGN Deutsches Gesundheitsnetz

d. h. das heißt

DIN Deutsche Industrienorm

DONot Dienstordnung für Notarinnen und Notare

DONotI-Report Deutsches Notarinstitut[-Report] (Zeitschrift)

DONotZ Deutsche Notar-Zeitschrift

DSA Digital Signature Algorithm

DSGVO Datenschutz-Grundverordnung

DSS CEF Digital Signature Services

DStR Deutsches Steuerrecht (Zeitschrift)

DuD Zeitschrift für Datenschutz und Datensicherheit

ECDSA Elliptic Curve Digital Signature Algorithm

eIDAS electronic IDentification, Authentication and trust Services

ErbR Zeitschrift für die gesamte erbrechtliche Praxis

Erwgr Erwägungsgrund

etc. et cetera

EU	Europäische Union
EuGH	Europäischer Gerichtshof
e. V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
f.	und folgende Seite
FamFG	Familienverfahrensgesetz
FamR	Familienrecht
FamRZ	Zeitschrift für das gesamte Familienrecht
FD-ErbR	Zeitschrift für die gesamte erbrechtliche Praxis
ff.	und folgende Seiten
FGPrax	Praxis der Freiwilligen Gerichtsbarkeit (Zeitschrift)
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standard
FPR	Familie Partnerschaft Recht (Zeitschrift)
FS Fezer	Festschrift für Karl-Heinz Fezer zum 70. Geburtstag
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GKG	Gerichtskostengesetz
GNotKO	Gerichts- und Notarkostengesetz
GRCh	Charta der Grundrechte der Europäischen Union
GRUR-Praxis	Gewerblicher Rechtsschutz und Urheberrecht. Praxis im Immaterialgüter- und Wettbewerbsrecht (Zeitschrift)
GVG	Gerichtsverfassungsgesetz
Hrsg.	Herausgeber
HSM	Hardware Security Module
HTML	Hypertext Markup Language
IADIS	International Association for Development of the Information Society (Konferenz)
IL	Israel (Länderkürzel)
InsO	Insolvenzordnung

I. S. d.	im Sinne des
ISO	International Organization for Standardization
IT	Informationstechnik
I. V. m.	in Verbindung mit
JZ	JuristenZeitung (Zeitschrift)
KUG	Kunsturhebergesetz
LG	Landgericht
lit.	Littera, Buchstabe
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
MIME	Multipurpose Internet Mail Extensions
MitBayNot	Mitteilungen des Bayerischen Notarvereins, der Notarkasse und der Landesnotarkammer Bayern (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
MRZ	Machine Readable Zone
MükoBGB	Münchener Kommentar zum Bürgerlichen Gesetzbuch
m. w. N.	mit weiteren Nachweisen
NISTIR	National Institute of Standards and Technology Interagency Report
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJWE-FER	NJW-Entscheidungsdienst Familien- und Erbrecht (Zeitschrift)
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report Zivilrecht (Zeitschrift)
NotBZ	Zeitschrift für die notarielle Beratungs- und Beurkundungspraxis
Nr.	Nummer
NWB	Neue Wirtschafts-Briefe (Verlag)
NWB-EV	NWB Erben und Vermögen
NZFam	Neue Zeitschrift für Familienrecht
OCR	Optical Character Recognition
o. g.	oben genannt(e/n)
OLG	Oberlandesgericht
PAuswG	Personalausweisgesetz

PAuswV	Personalausweisverordnung
PDF/A	Portable Document Format for Archiving
PIN	Personal Identification Number
PKI	Public-Key-Infrastruktur
PoW	Proof-of-Work
PStG	Personenstandsgesetz
PStV	Personenstandsverordnung
ptble	Projektträger Bundesanstalt für Landwirtschaft und Ernährung
PUK	Personal Unblocking Key
PVDA	Plattform zur Vererbung von Digitalen Accounts
QES	Qualifizierte Elektronische Signatur
QR-Code	Quick Response Code
RESTful	Representational State Transfer
RFC	Request For Comments
Rn.	Randnummer
RNotZ	Rheinische Notar-Zeitschrift
RSA	Rivest, Shamir and Adleman (Algorithmus)
S.	Seite/Satz (nach Paragraph)
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SE	Schweden (Länderkürzel)
SIGSAC	ACM Special Interest Group on Security, Audit and Control (Konferenz)
SIM	Subscriber Identity Module
SMS	Short Message Service
SSO	Single Sign-On
TAN	Transaktionsnummer
TC	Technical Committee
TLS	Transport Layer Security
TMG	Telemediengesetz

TOTP	Time-based One-time Password
TR	Technische Richtlinie
u. a.	unter anderen/unter anderem
UK	Vereinigtes Königreich Großbritannien und Nordirland (Länderkürzel)
UrhG	Urhebergesetz
URL	Uniform Resource Locator
Urt.	Urteil
US	Vereinigten Staaten von Amerika (Länderkürzel)
USB	Universal Serial Bus
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
U2F	Universal Second Factor
vgl.	vergleiche
VO	Verordnung
VuR	Verbraucher und Recht (Zeitschrift)
WG	Working Group (Standardisierung)
xAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZErb	Zeitschrift für die Steuer- und Erbrechtspraxis
ZEV	Zeitschrift für Erbrecht und Vermögensnachfolge
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht

Literatur

Adhikari, Sandeep (2012). *Digital Afterlife: A General Overview*. Hrsg. von Oulu University of Applied Sciences.

Amend-Traut, Anja und Cyril Hergenröder (2019). “Kryptowährungen im Erbrecht”. In: *ZEV*, S. 113–121.

Arbeitsgruppe Digitaler Neustart der Konferenz der Justizministerinnen und Justizminister der Länder (Mai 2017). *Bericht vom 15. Mai 2017 unter Mitwirkung der Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen (Federführung), Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein*.

Bamberger, Georg u. a., Hrsg. (2019). *Beck’scher Onlinekommentar BGB*. 51. Edition. München.

Bamberger, Heinz Georg u. a., Hrsg. (2019). *Beck’scher Onlinekommentar BGB*. 50. Edition. C.H. Beck.

Bär, Christian, Thomas Grädler und Robert Mayr, Hrsg. (2018). *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht*. 1. Auflage. Bd. Band 1 – Politik und Wirtschaft. Springer.

Berentsen, Aleksander und Fabian Schär (2017). *Bitcoin, Blockchain und Kryptoassets – Eine umfassende Einführung*. Universität Basel: Berentsen, Aleksander und Schär, Fabian.

Berghoff, Christian u. a. (2019). *Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen*. Techn. Ber. Bundesamt für Sicherheit in der Informationstechnik (BSI).

Berkl, Melanie (2015). *Personenstandsrecht. Handbuch zu System und Anwendung*. Frankfurt am Main, Berlin: Verlag für Standesamtswesen.

Bleich, Holger (2013). “Ableben 2.0”. In: *c’t* 2, S. 62–64.

Brandão, Luís T. A. N., Nicky Mouha und Apostol Vassilev (2019). *NISTIR 8214 – Threshold Schemes for Cryptographic Primitives – Challenges and Opportunities in Standardization and Validation of Threshold Cryptography*. Techn. Ber. National Institute of Standards and Technology.

Bräutigam, Peter (2012). “Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten”. In: *MMR*, S. 635–641.

Bräutigam, Peter und Daniel Rücker (2016). *E-Commerce: Rechtshandbuch*. Hrsg. von Peter Bräutigam und Daniel Rücker. C.H. Beck.

Brink, Stefan und Heinrich Amadeus Wolff, Hrsg. (2019). *Beck'scher Onlinekommentar Datenschutzrecht*. 29. Edition. München.

Brisch, Klaus und Marco Müller-ter Jung (2013). "Digitaler Nachlass – Das Schicksal von E-Mail- und De-Mail-Accounts sowie Mediencenter-Inhalten". In: *CR*, S. 446–455.

Brucker-Kley, Elke, Thomas Keller, Lukas Kurtz, Kurt Pärli, Claudia Pedron u. a. (2013). "Passing and Passing on in the Digital World – Issues and Solutions for the Digital Estate". In: *IADIS International Conference on e-Society 2013, Lisbon, Portugal, 13.–16. March 2013*. IADIS, S. 248–256.

Brucker-Kley, Elke, Thomas Keller, Lukas Kurtz, Kurt Pärli, Matthias Schweizer u. a. (2013). *Sterben und Erben in der digitalen Welt: von der Tabuisierung zur Sensibilisierung: Crossing Borders: Ergebnisse eines interdisziplinären Forschungsprojekts*. Hrsg. von ZHAW School of Management and Law. vdf Hochschulverlag.

Buchner, Benedikt (2019). "Von der Wiege bis zur Bahre? – Datenschutz im Familienrecht unter der DS-GVO". In: *FamRZ*, S. 665–671.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Mai 2018). *Technische Richtlinie TR-03127 – eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control – Personalausweis und elektronischer Aufenthaltstitel, Version 1.21*.

– (Mai 2019). *Technische Richtlinie TR-03107-1 – Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen, Version 1.1.1*.

Burandt, Wolfgang und Dieter Rojahn, Hrsg. (2019). *Erbrecht*. 3. Auflage. Bd. Band 65. Beck'sche Kurz-Kommentare. München.

Büscher, Wolfgang u. a. (2016). *Festschrift für Karl-Heinz Fezer zum 70. Geburtstag*. C.H. Beck.

Datenethikkommission der Bundesregierung (Okt. 2019). *Gutachten der Datenethikkommission der Bundesregierung*. Techn. Ber. Bundesministerium des Innern, für Bau und Heimat; Bundesministerium der Justiz und für Verbraucherschutz.

Deinert, Horst und Kay Lütgens (2009). "Betreuung und Postverkehr". In: *BtPrax*, S. 212–217.

Determann, Lothar (2018). "Gegen Eigentumsrechte an Daten". In: *ZD*, S. 503–508.

Dethloff, Nina (2018). *Familienrecht*. 32. Auflage. München: C.H. Beck.

Deusch, Florian (2014). "Digitales Sterben: Das Erbe im Web 2.0". In: *ZEV*, S. 2–8.

– (2018). "Der digitale Nachlass vor dem BGH und die Praxisfolgen". In: *ZEV*, S. 687–691.

Deutscher Anwaltverein (Juni 2013). *Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht zum Digitalen Nachlass – Stellungnahme Nr.: 34/2013*.

Diehn, Thomas und Ralf Rebhan (2010). "Vorsorgevollmacht und Patientenverfügung". In: *NJW*, S. 326–331.

Dodegge, Georg und Andreas Roth (2018). *Systematischer Praxiskommentar Betreuungsrecht*. 5. Auflage. Köln: Bundesanzeiger Verlag.

Eagleman, David (2006). “A brief History of Death Switches”. In: *Nature 443, 882*.

Edwards, Lilian und Edina Harbina (2013). “Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World”. In: *Cardozo Arts & Ent. LJ* 32, S. 83.

Edwards, Lilian und Edina Harbinja (2013). “‘What Happens to My Facebook Profile When I Die?’ – Legal Issues Around Transmission of Digital Assets on Death”. In: *Digital legacy and interaction*. Springer, S. 115–144.

Engelbertz, Nils u. a. (2019). “Security Analysis of XAdES Validation in the CEF Digital Signature Services (DSS)”. In: *Open Identity Summit 2019*, S. 95–106.

Ensthaler, Jürgen (2016). “Industrie 4.0 und die Berechtigung an Daten”. In: *NJW*, S. 3473–3478.

Funk, Stephanie (2017). *Das Erbe im Netz: Rechtslage und Praxis des digitalen Nachlasses*. Springer.

Gaaz, Berthold und Heinrich Bornhofen (2014). *Personenstandsgesetz Handkommentar*. 3. Auflage. Frankfurt am Main, Berlin: Verlag für Standesamtswesen.

Ghasemisharif, Mohammad u. a. (2018). “O Single Sign-off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web”. In: *27th USENIX Security Symposium*, S. 1475–1492.

Gloser, Stefan (2015). “‘Digitale Vorsorge’ in der notariellen Praxis”. In: *DNotZ*, S. 4–20.

– (2016a). “‘Digitale Erblasser’ und ‘digitale Vorsorgefälle’ – Herausforderungen der Online-Welt in der notariellen Praxis – Teil I”. In: *MittBayNot*, S. 12–19.

– (2016b). “‘Digitale Erblasser’ und ‘digitale Vorsorgefälle’ – Herausforderungen der Online-Welt in der notariellen Praxis – Teil II”. In: *MittBayNot*, S. 101–108.

Gola, Peter, Hrsg. (2018). *DS-GVO/Kommentar zur DS-GVO*. 2. Auflage. München.

Gomille, Christian (2018). “Information als Nachlassgegenstand”. In: *Zeitschrift für Urheber- und Medienrecht*.

Groll, Klaus-Michael und Anton Steiner (2019). *Praxis-Handbuch Erbrechtsberatung*. 5. Auflage. Köln.

Grützmacher, Malte (2016). “Dateneigentum – ein Flickenteppich – Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?” In: *CR*, S. 485–495.

Gsell, Beate u. a., Hrsg. (2019). *beck-online.GROSSKOMMENTAR BGB*. C.H. Beck.

Günther, Thomas (2013). “Legitimationsprüfungen bei Erben, Betreuern und Bevollmächtigten”. In: *NJW*, S. 3681–3686.

Halfmeier, Axel (2017). “Musterfeststellungsklage: Nicht gut, aber besser als nichts”. In: *ZPR*, S. 201–204.

Hansen, Marit (2009). “Putting Privacy Pictograms into Practice – a European Perspective”. In: *INFORMATIK 2009 – Im Focus das Leben, Beitrage der 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI)* 154, S. 1703–1716.

Hansen, Marit und Angelika Martin (2019). “Ein Schritt zur Verbesserung der Transparenz für alle – der Datenschutz-Steckbrief”. In: *BvD-News* 2, S. 64–66.

Harbinja, Edina (2017). “Post-mortem Privacy 2.0: Theory, Law, and Technology”. In: *International Review of Law, Computers & Technology* 31.1, S. 26–42.

Hasil, Cornelia (2017). “Digitaler Nachlass – Anleitung zur rechtlich korrekten Abhandlung im Web 2.0”. Magisterarb. Fakultät für Informatik der Technischen Universität Wien.

Hausmann, Rainer und Gerhard Hohloch, Hrsg. (2010). *Handbuch des Erbrechts*. 2. Auflage. Berlin.

Heinemann, Daniela und Manuel Heinemann (2013). “Postmortaler Datenschutz”. In: *DuD*, S. 242–245.

Heintschel-Heinegg, Bernd, Hrsg. (2011). *Münchener Kommentar zum Strafgesetzbuch*.

Hergenröder, Cyril H. (2018). “Testieren 2.0: Errichtung eines digitalen eigenhändigen Testaments mittels Touch- oder Smartpen?” In: *ZEV*, S. 7–11.

Herzog, Stephanie (2013). “Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem”. In: *NJW*, S. 3745–3751.

Herzog, Stephanie und Matthias Pruns (2018). *Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis*. 1. Auflage. Bonn: NWB Verlag.

Heymann, Thomas (2016). “Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen”. In: *CR*, S. 650–657.

Hilty, Reto M. (2018). “Kontrolle der digitalen Werknutzung zwischen Vertrag und Erschöpfung”. In: *Gewerblicher Rechtsschutz und Urheberrecht*, S. 856–880.

Hoeren, Thomas (2005). “Der Tod und das Internet – Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers”. In: *NJW*, S. 2113–2117.

Hoeren, Thomas, Ulrich Sieber und Bernd Holznagel (2018). *Handbuch Multimedia-Recht*. C.H. Beck.

Hopkins, Jamie P (2013). “Afterlife in the Cloud: Managing a Digital Estate”. In: *Hastings Sci. & Tech. LJ* 5, S. 209.

Jandt, Silke und Roland Steidle, Hrsg. (2018). *Datenschutz im Internet – Rechtshandbuch zu DSGVO und BDSG*.

Jurgeleit, Andreas, Hrsg. (2018). *Betreuungsrecht Handkommentar*. 4. Auflage. Baden-Baden.

Keidel, Theodor, Hrsg. (2017). *FamFG Kommentar*. 19. Auflage. München.

Klas, Benedikt und Christine Möhrke-Sobolewski (2015). “Digitaler Nachlass – Erbenschutz trotz Datenschutz”. In: *NJW*, S. 3473–3478.

Kneese, Tamara (2019). “Networked Heirlooms: the Affective and Financial Logics of Digital Estate Planning”. In: *Cultural Studies* 33.2, S. 297–324.

Koreng, Ansgar und Matthias Lachenmann (2018). *Formularhandbuch Datenschutzrecht*. C.H. Beck.

Kroiß, Ludwig, Claus-Henrik Horn und Dennis Solomon, Hrsg. (2019). *Nachfolgerecht Erbrechtliche Spezialgesetze*. 2. Auflage. Baden-Baden.

Kropp, Gabriela (2012). “Die Vorsorgevollmacht”. In: *FPR*, S. 9–13.

Kühling, Jürgen und Benedikt Buchner (2017). *Datenschutz-Grundverordnung Kommentar*. C.H. Beck.

Kühling, Jürgen, Mario Martini u. a. (2016). *Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf*. 1. Auflage. Monsenstein und Vannerdat.

Kühling, Jürgen, Christian Seidel und Anastasios Sivridis (2011). *Datenschutzrecht*. C.F. Müller.

Kutscher, Antonia (2015). “Der digitale Nachlass”. Diss. Göttingen.

Kwoska, Adam (2018). “Digitaler Nachlass – ein Aspekt der Techniksouveränität”. In: *Partizipative Technikentwicklung: Methodik und Umsetzungsbeispiele, Handbuchreihe “Ältere als (Ko-)Produzenten von Quartiersnetzwerken – Impulse aus dem Projekt QuartiersNETZ”, No. 4*. Hrsg. von Andreas Diepenbrock, Jonas Sorgalla und Sabine Sachweh. Fachhochschule Dortmund und Forschungsinstitut Geragogik, Dortmund. Kap. 5, S. 73–82.

Lange, Knut Werner und Marian Holtwiesche (2016). “Das digitale Erbe – eine rechtstatsächliche Bestandsaufnahme”. In: *ErbR*, S. 487–492.

– (2018). “Der digitale Nachlass”. In: *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht*. Springer, S. 103–117.

Lieder, Jan und Daniel Berneith (2018). “Digitaler Nachlass: Das Facebook-Urteil des BGH”. In: *FamRZ*, S. 1486–1488.

Litzenburger, Wolfgang (2018). “BGH: Digitale Benutzerkonten sind vererblich Urteilsanmerkung”. In: *FD-ErbR*, S. 407688.

Löhnig, Martin (2006). *Treuhand – Interessenwahrnehmung und Interessenkonflikte*. Tübingen: Mohr Siebeck.

– (2011). “Vorsorgevollmacht und Erwachsenenschutz in Europa”. In: Hrsg. von Martin Löhnig u. a. Beiträge zum europäischen Familienrecht 13. Bielefeld: Gieseking. Kap. Probleme der Vorsorgevollmacht nach deutschem Recht, S. 15–26.

Lopes, Aron Daniel, Cristiano Maciel und Vinicius Carvalho Pereira (2014). “Virtual Homage to the Dead: An Analysis of Digital Memorials in the Social Web”. In: *Social Computing and Social Media*. Hrsg. von Gabriele Meiselwitz. Cham: Springer International Publishing, S. 67–78.

Lydiga, Hannes (2018). “‘Digitales Update’ für das Erbrecht im BGB?” In: *ZEV*, S. 1–6.

Maciel, Cristiano und Vinicius Carvalho Pereira (2012). “The Internet Generation and its Representations of Death: Considerations for Posthumous Interaction Projects”. In: *Proceedings of the 11th Brazilian Symposium on Human Factors in Computing Systems*. Brazilian Computer Society, S. 85–94.

– (2013). “Social Network Users’ Religiosity and the Design of Post Mortem Aspects”. In: *IFIP Conference on Human-Computer Interaction*. Springer, S. 640–657.

– (2016). “Technological and Human Challenges to Addressing Death in Information Systems”. In: *I GranDSI-BR*, S. 161.

Maciel, Cristiano, Vinicius Carvalho Pereira und Monica Sztern (2015). “Internet Users’ Legal and Technical Perspectives on Digital Legacy Management for Post-mortem Interaction”. In: *Human Interface and the Management of Information. Information and Knowledge Design*. Hrsg. von Sakae Yamamoto. Cham: Springer International Publishing, S. 627–639.

Manegold, Bartholomäus und Ilja Czernik (2014). “§ 95 Laufbilder”. In: *Praxiskommentar zum Urheberrecht*. Hrsg. von Artur-Axel Wandtke und Winfried Bullinger. Bd. 4. Auflage.

Markendorf, Merih (2018). “Recht an Daten in der deutschen Rechtsordnung – Blockchain als Lösungsansatz für eine rechtliche Zuordnung?” In: *ZD*, S. 409–413.

Martini, Mario (2012). “Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet”. In: *JuristenZeitung* 67.23, S. 1145–1155.

– (2013). “‘Wenn ich einmal soll scheiden ...’: Der digitale Nachlass und seine unbewältigte rechtliche Abwicklung”. In: *Facebook, Google & Co.* Nomos Verlagsgesellschaft, S. 77–126.

Martini, Mario und Thomas Kienle (2019). “Facebook, die Lebenden und die Toten”. In: *JZ*, S. 235–241.

McKinnon, Laura (2011). “Planning for the Succession of Digital Assets”. In: *Computer Law & Security Review* 27.4, S. 362–367.

Micklitz, Stephan, Martin Ortlieb und Jessica Staddon (2013). “‘I hereby leave my email to ...’: Data Usage Control and the Digital Estate”. In: *2013 IEEE Security and Privacy Workshops*. IEEE, S. 42–44.

Mladenov, Vladislav u. a. (2019). “1 Trillion Dollar Refund: How to Spoof PDF Signatures”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’19. London, United Kingdom: ACM, S. 1–14.

Müller-Engels, Hrsg. (2019). *beck-online Großkommentar zum Beurkundungsgesetz*. München.

Müller-Engels, Gabriele und Thomas Renner (2018). *Betreuungsrecht und Vorsorgeverfügungen in der Praxis*. 5. Auflage. Köln.

Müller, Gabriele (2015). “Update Betreuungsrecht – Aktuelle Fragen rund um Betreuung und Vorsorgevollmacht”. In: *DNotZ*, S. 403–417.

Müller, Gabriele und Thomas Renner, Hrsg. (2018). *Betreuungsrecht und Vorsorgeverfügungen in der Praxis*. 5. Auflage. Köln.

Nagel, Emily van der u. a. (2017). *Death and the Internet – Consumer Issues for Planning and Managing Digital Legacies (2nd edition)*. Techn. Ber. University of Melbourne.

Nellius, Lena, Robert Zepic und Helmut Krcmar (2019). “Finaler Logout – ein neuer Ansatz für die Gestaltung des digitalen Nachlasses bei sozialen Netzwerken”. In: *Digitalisierung von Staat und Verwaltung*, S. 37–48.

Niebling, Jürgen, Hrsg. (2014). *AnwaltKommentar AGB-Recht*. Deutscher Anwaltverlag & Institut der Anwaltschaft GmbH.

Notarinstitut, Deutsches (2013). “Vorsorgevollmacht; Berechtigung zur Entgegennahme der Post; BGB § 1896 Abs. 2 und 4”. In: *DNotI-Report*, S. 148–150.

Odom, William u. a. (2012). “Technology Heirlooms? – Considerations for Passing Down and Inheriting Digital Materials”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. New York, NY, USA: ACM, S. 337–346.

Paal, Boris und Daniel Pauly (2017). *Datenschutz-Grundverordnung – Kompakt-Kommentar*. C.H. Beck.

Palandt, Otto, Hrsg. (2019). *Bürgerliches Gesetzbuch*. 78. Auflage. München.

Peschel, Christopher und Sebastian Rockstroh (2014). “Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste”. In: *MMR*, S. 571–576.

Pfister, Joachim (2017). “‘This Will Cause a Lot of Work.’: Coping with Transferring Files and Passwords As Part of a Personal Digital Legacy”. In: *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. CSCW ’17. ACM, S. 1123–1138.

Pfister, Joachim und Gerhard Schwabe (2013). “The Landscape of Electronic Data Safes and their Adoption in E-Government and E-Business”. In: *2013 46th Hawaii International Conference on System Sciences*. IEEE, S. 1963–1972.

Phelps, Charles (2014). “More Inheritable Rights for Digital Assets”. In: *Rutgers L. Rec.* 41, S. 131–133.

Pimminger, Sebastian u. a. (Apr. 2015). *Themis – Conserve Your Digital Life*. Techn. Ber. FFH2015-CBS1-3.

Preuß, Nicola (2018). “Digitaler Nachlass – Vererbbarkeit eines Kontos bei einem sozialen Netzwerk”. In: *NJW*, S. 3146–3149.

Pruns, Matthias (2013). “Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?” In: *NWB*, S. 3161–3167.

– (2018). “Der digitale Nachlass in der Beratungspraxis nach dem Facebook-Urteil des BGH. Teil 2: Soziale Netzwerke – Rechtliche Durchsetzung – Vorsorge”. In: *ErbR*, S. 614–622.

Raude, Karin (2017). “Der digitale Nachlass in der notariellen Praxis”. In: *RNotZ*, S. 17–27.

Rauscher, Thomas, Hrsg. (2019). *Münchner Kommentar zum FamFG*. 3. Auflage. Bd. Band 2: §§ 271–493 Internationales und Europäisches Zivilverfahrensrecht in Familiensachen. München.

Reimann, Wolfgang, Manfred Bengel und Jörg Mayer, Hrsg. (2015). *Testament und Erbvertrag*. 6. Auflage. Köln.

Rott, Eberhard und Alexander Rott (2013). “Wem gehört die E-Mail? Rechts- und Praxisprobleme beim digitalen Nachlass”. In: *NWB-EV*, S. 160–168.

Säcker, Franz Jürgen u. a., Hrsg. (2018). *Münchner Kommentar zum Bürgerlichen Gesetzbuch*. 8. Auflage. Bd. Band 1 – Allgemeiner Teil. C.H. Beck.

– Hrsg. (2020a). *Münchner Kommentar zum Bürgerlichen Gesetzbuch*. 8. Auflage. Bd. Band 9: §§ 1589–1921 BGB, SGB VIII. C.H. Beck.

– Hrsg. (2020b). *Münchner Kommentar zum Bürgerlichen Gesetzbuch*. 8. Auflage. Bd. Band 10: Erbrecht §§ 1922–2385, §§ 27–35 BeurkG.

Salomon, Pascal (2016). “‘Digitaler Nachlass’ – Möglichkeiten der notariellen Vorsorge”. In: *NotBZ*, S. 324–331.

Schaeffter, Markus (2016). *Verfahrensverzeichnis 2.0 – Datenschutzdokumentation konform zur EU-Datenschutzgrundverordnung gestalten*.

Scherer, Stephan, Hrsg. (2018). *Münchener Anwaltshandbuch Erbrecht*. 5. Auflage. München.

Schleifenbaum, Thekla (2015). “Wann sollte ich Testamentsvollstreckung anordnen? Teil 2: Besondere Gründe für Testamentsvollstreckung bei Unternehmensbeteiligungen, Sonderfälle”. In: *ErbR*, S. 230–237.

Schlund, Albert und Hans Pongratz (2018). “Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung”. In: *DStR*, S. 598–604.

Schmid, Claus u. a. (2013). “Sterben im Internet – Regelung des digitalen Nachlasses”. In: *Wirtschaftsinformatik & Management* 5.1, S. 86–96.

Scholz, Philipp (2019a). “Digitales Testieren. Zur Verwendung digitaler Technologien beim eigenhändigen und Nottestament de lege lata et ferenda”. In: *AcP*, S. 100–137.

– (2019b). “Zulässigkeit und Grenzen der Verwendung digitaler Technologien beim Testieren”. In: *ErbR*, S. 617–621.

Schönke, Adolf und Horst Schröder, Hrsg. (2019). *Strafgesetzbuch Kommentar*. C.H. Beck.

Schwab, Martin (2018). *AGB-Recht (Recht in der Praxis)*. C.F. Müller.

Schweitzer, Heike und Martin Peitz (2018). “Ein neuer europäischer Ordnungsrahmen für Datenmärkte”. In: *NJW*, S. 275–280.

Seidler, Katharina (2016). *Digitaler Nachlass – Das postmortale Schicksal elektronischer Kommunikation*. 1. Auflage. Frankfurt: Wolfgang Metzner Verlag.

Simits, Spiros, Gerrit Hornung und Indra Spiecker genannt Döhmann, Hrsg. (2019). *Datenschutzrecht DSGVO mit BDSG*. 1. Auflage. Baden-Baden.

Soergel, Hans-Theodor, Hrsg. (2002). *Soergel Kommentar zum Bürgerlichen Gesetzbuch*. 13. Auflage. Bd. Band 22 – Erbrecht 2. Stuttgart.

Solmecke, Christian, Thomas Köbrich und Robin Schmitt (2015). “Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen”. In: *MMR*, S. 291–295.

Sorge, Christoph (2018). “Digitaler Nachlass als Knäuel von Rechtsverhältnissen – Justizministerkonferenz sieht kaum Handlungsbedarf für den Gesetzgeber”. In: *MMR*, S. 372–377.

Specht, Louisa (2016). “Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen”. In: *CR*, S. 288–296.

Spindler, Gerald und Fabian Schuster (2019). *Recht der elektronischen Medien*. C.H. Beck.

Stadler, Astrid (2018). “Musterfeststellungsklagen im deutschen Verbraucherrecht?” In: *VuR*, S. 83–89.

Staudinger, Julius von (2014). *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen*. Bd. Buch 1 – Allgemeiner Teil.

– (2017a). *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen*. Bd. Buch 5 – Erbrecht.

– (2017b). *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen*. Bd. Buch 4 – Familienrecht §§ 1896-1921.

Steiner, Anton und Anna Holzer (2015). “Praktische Empfehlungen zum digitalen Nachlass”. In: *Zeitschrift für Erbrecht und Vermögensnachfolge* 5.15, S. 262–266.

Stieper, Malte (2019). “Urheberrecht in der Cloud”. In: *Zeitschrift für Urheber- und Medienrecht*, S. 1–7.

Streubel, Denise (2019). *Der Digitale Nachlass – Probleme, Konzepte und Praxen*. Techn. Ber. Universität Leipzig – Fakultät für Mathematik und Informatik.

Taeger, Jürgen u. a., Hrsg. (2018). *Computerrechts-Handbuch*. 34. Ergänzungslieferung. C.H. Beck.

Thalhofer, Thomas (2017). “Recht an Daten in der Smart Factory”. In: *GRUR-Prax*, S. 225–227.

Uhrenbacher, Pia (2018). “Rechtsprobleme des digitalen Nachlasses im Hinblick auf Pflichtteilsansprüche und Testamentsvollstreckung”. In: *ZEV*, S. 248–251.

View, Mountain u. a. (Mai 2011). *TOTP: Time-Based One-Time Password Algorithm*. RFC 6238.

Waclawik, Erich (2018). “Die Musterfeststellungsklage”. In: *NJW*, S. 2921–2926.

Walorska, Agnieszka Maria und Marie-Luise Jaeger (2014). “Der digitale Tod – Herausforderungen an die User Experience”. In: *UP14-Vorträge*.

Wandtke, Artur-Axel und Winfried Bullinger (2014). *Praxiskommentar zum Urheberrecht*. Hrsg. von Artur-Axel Wandtke und Winfried Bullinger. C.H. Beck.

Wende, Holger (März 2019). “Digitaler Nachlass – wie wir präventiv Regelungslücken vermeiden”. In: *Schmerzmedizin* 35.2, S. 54–56.

Werkmüller, Maximilian (2000). “Vollmacht und Testamentsvollstreckung als Instrumente der Nachfolgegestaltung bei Bankkonten”. In: *ZEV*, S. 305–308.

Werner, Rüdiger (2019). “Trans- und postmortale Vollmachten als Instrument der Vermögensnachfolge”. In: *ZErb*, S. 137–142.

Westermann, Harm Peter, Barbara Grundewald und Georg Maier-Reimer, Hrsg. (2017). *Erman Bürgerliches Gesetzbuch Handkommentar*. 15. Auflage. Bd. Band I. Köln.

Wiebe, Andreas und Nico Schur (2017). “Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit”. In: *ZUM*, S. 461–473.

Willems, Constantin (2016). “Erben 2.0 – zur Beschränkbarkeit der Rechtsnachfolge in das ‘digitale Vermögen’”. In: *ZfPW*, S. 494–512.

Wolff, Heinrich Amadeus und Stefan Brink, Hrsg. (2019). *Beck’scher Onlinekommentar Datenschutzrecht*. 29. Edition. München.

Zech, Herbert (2015). “Daten als Wirtschaftsgut – Überlegungen zu einem ‘Recht des Datenerzeugers’ – Gibt es für Anwenderdaten ein eigenes Vermögensrecht bzw. ein übertragbares Ausschließlichkeitsrecht?” In: *CR*, S. 137–146.

Obwohl sich jeder Mensch in seinem Leben zwangsläufig mit den Themen des Erbens und Vererbens beschäftigen muss, ist nur wenigen Menschen überhaupt bewusst, dass das Erbe auch aus digitalen Werten – dem sogenannten „digitalen Nachlass" – bestehen kann. Selbst Menschen, die sich dieser Tatsache bewusst sind, treffen i. d. R. keinerlei Vorkehrungen für ihre digitalen Werte, obwohl dies aus Sicht des Erblassers – also aus Sicht des Menschen, der Vorsorge für seinen Todesfall treffen möchte – dringend anzuraten ist. Vor diesem Hintergrund hat sich die vorliegende Studie zum Ziel gesetzt, das Thema des digitalen Nachlasses aufzuarbeiten. Im Fokus stehen hierbei erbrechtliche, datenschutzrechtliche, verbraucherschutzrechtliche und technische Fragestellungen.