Backup und Archivierung rechtssicher betreiben

Ausgezeichnet aufgezeichnet

Joerg Heidrich

Das Verarbeiten und Speichern der Daten von Kunden und Mitarbeitern ist für Unternehmen essenziell. Dennoch sind Schlampereien bei der Durchführung von Backups immer noch üblich. Auf der anderen Seite gibt es ein starkes Bedürfnis, auch persönliche Informationen möglichst lange zu speichern und lückenlos auszuwerten. Beiden Extremen jedoch stehen die strengen Vorgaben des Datenschutzes entgegen. Was bei Speicher- und Löschkonzepten zu beachten ist.

Sei es als vorübergehendes Backup von Logfiles oder als Langzeitspeicherung im Rahmen der E-Mail-Archivierung: Die Sicherung von Daten ist für Unternehmen in vielen Bereichen nicht nur sinnvoll, sondern sogar rechtlich vorgeschrieben. Allerdings hat diese private „Vorratsdatenspeicherung" auch rechtliche Grenzen. Diese beziehen sich sowohl darauf, was gespeichert werden soll und muss, als auch vor allem auf die Frage, wie lange die Informationen vorgehalten werden dürfen.

Rechtliche Vorgaben gibt es vor allem dann, wenn es sich dabei um sogenannte personenbezogene Daten handelt. Darunter versteht Paragraf 3 des Bundesdatenschutzgesetzes (BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Es geht also um diejenigen Informationen, auf deren Basis Menschen identifiziert werden können. Dazu zählen etwa Name, Adresse, Geburtsdatum und vergleichbare Angaben, aber etwa auch genetische Daten oder IP-Adressen.

Informationen über Kunden und die eigenen Mitarbeiter sowie E-Mails fallen daher immer unter die Vorgaben des Datenschutzes. Etwas anderes gilt beispielsweise für technische Daten, Konstruktionspläne oder Maschinenauswertungen. Derartige Informationen ohne Personenbezug kann man aus juristischer Sicht in den allermeisten Fällen unbeschränkt speichern und vorhalten. Allerdings können sich auch in solchen Archiven Löschpflichten verstecken, etwa wenn Lizenzvereinbarungen auslaufen oder nach Vertragsende Daten eines Vertragspartners zwingend gelöscht werden müssen.

Erlaubnis benötigt

Handelt es sich aber um personenbezogene Daten – dafür reichen auch einzelne Informationen in einer größeren Datenmenge –, sind die rechtlichen Vorgaben des Datenschutzes zu beachten. Danach dürfen solche Informationen grundsätzlich nur verarbeitet und gespeichert werden, wenn dafür eine Einwilligung aller Betroffenen oder eine gesetzliche Erlaubnis vorliegt. Einwilligungen sind in diesem Bereich eher selten, aber rechtlich möglich. Voraussetzung ist, dass der Nutzer vor Erhebung über das Schicksal seiner Daten informiert wird und in dieser Kenntnis der Speicherung der Daten zustimmt.

Wer zum Beispiel in die Zusendung eines Newsletters einwilligt, stimmt damit zugleich zwingend der zeitlich unbegrenzten Speicherung seiner Mailadresse zu. Diese Erlaubnis gilt im Zweifelsfall so lange, bis der Nutzer sein Abonnement abbestellt, der Speicherung seiner Daten explizit widerspricht oder bis das Projekt eingestellt wird. In allen Fällen muss allerdings gewährleistet sein, dass die Informationen über diesen Nutzer vollständig gelöscht werden – und zwar auch aus etwaigen Backups, was in der Praxis häufig vernachlässigt wird.

Im Regelfall gilt es jedoch, eine Rechtsgrundlage zu finden, auf deren Basis die Daten verarbeitet werden können. Solche Erlaubnistatbestände finden sich zahlreich im BDSG selbst. So regelt Paragraf 32 die „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses". Danach ist in einem Arbeitsverhältnis die Nutzung von Mitarbeiterdaten erlaubt, soweit dies „für die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist".

Beispiel E-Mail-Archivierung

Die Langzeitspeicherung solcher Informationen kann dann im Einzelfall sogar zwingend erforderlich sein, etwa im Bereich der Gehaltszahlungen. Nach dem Ende des Beschäftigtenverhältnisses fällt diese Rechtsgrundlage wieder weg. An ihre Stelle können allerdings andere gesetzliche Erlaubnisse oder sogar Anforderungen zur Speicherung treten, etwa

im Bereich des Steuerrechts oder der Renten.

Welche Schwierigkeiten sich bei der praktischen Umsetzung juristischer Vorgaben ergeben können, zeigt seit vielen Jahren die Pflicht zur E-Mail-Archivierung. Diese findet ihre Grundlage in den Vorgaben der Abgabenordnung (AO) und des Handelsgesetzbuches (HGB). Danach müssen sämtliche steuerlich relevanten Daten in maschinell auswertbarer Form für die Dauer von bis zu zehn Jahren aufbewahrt und für einen Prüfzugriff aufbereitet werden. Zu diesen aufbewahrungspflichtigen Handelsbriefen gehören auch E-Mails und ihre Dateianhänge. Welche formalen technischen Voraussetzungen zu erfüllen sind, regeln die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD), die 2015 die GoBS ersetzt haben [1].

Damit fangen die rechtlichen Probleme allerdings erst an. Denn die Regelungen geben zwar ein verbindliches Speichern geschäftlicher E-Mails vor. Gleichzeitig verbieten aber Datenschutz und Arbeitsrecht zwingend die Archivierung rein privater Mails von oder an die Mitarbeiter. Zumindest in den Fällen, in denen den Mitarbeitern die private Nutzung der Mailzugänge gestattet ist, müssen solche persönlichen Nachrichten vor dem Archivieren zwingend von den Handelsbriefen getrennt werden. Dies ist, wenn überhaupt, nur mit einigem technischen oder tatsächlichen Aufwand möglich – zumindest wenn man den strengen Vorschriften der GoBD genügen will.

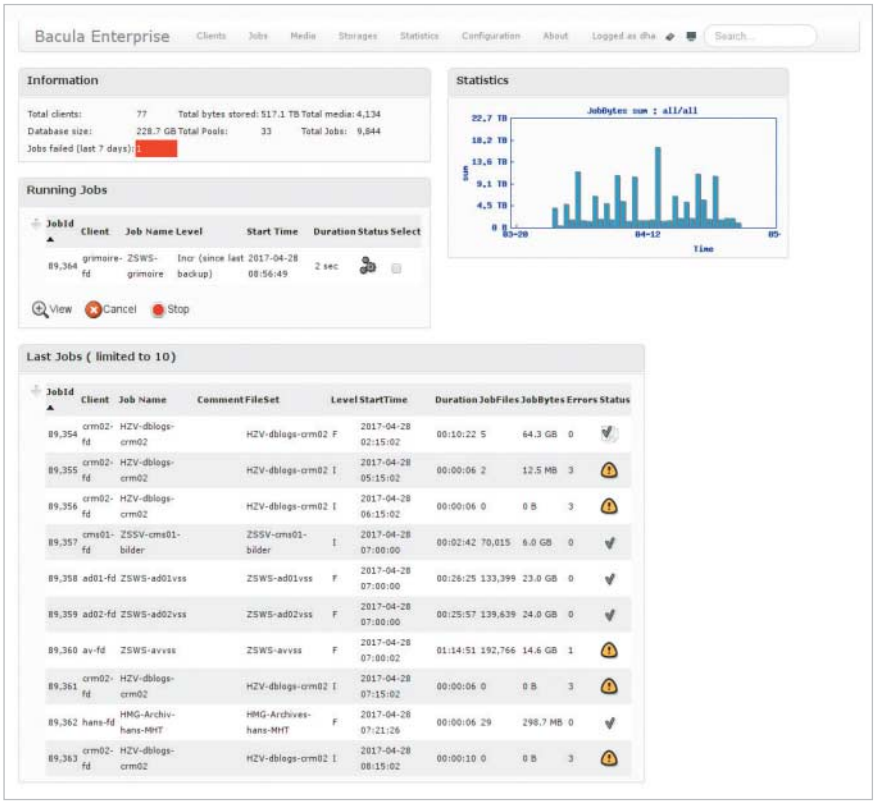
Nur zweckgebundene Speicherung

Eine weitere Hürde ist der eherne rechtliche Grundsatz der Zweckbindung. Danach dürfen Daten nur für den Zweck genutzt werden, zu dem sie gespeichert oder erfasst wurden. Für die steuerrechtlich begründete Archivierung von Handelsbriefen bedeutet dies, dass man eine solche Datensammlung eben nur für diesen Zweck benutzen darf. Die in vielen Unternehmen praktizierte zusätzliche Nutzung als E-Mail-Archiv und kurzfristiges Daten-Backup ist rechtlich unzulässig.

Ein anderer typischer Bereich für eine möglichst dauerhafte Speicherung von Daten betrifft die Backups, etwa von Logfiles. Im Regelfall werden hier in Form von IP-Adressen auch personenbezogene Daten erfasst. Rechtsprechung und gesetzliche Vorgaben sehen dafür eine Erlaubnis vor, soweit dies zu Zwecken der IT-Sicherheit erforderlich ist. Das bedeutet zunächst, dass „Nice to have“-Datensammlungen ebenso unzulässig sind wie eine Protokollierung zu Zwecken des Marketings. Auch eine spätere Nutzung dieser Informationen ist auf Basis der strengen Vorgaben der Zweckbindung nicht zulässig.

In der Praxis stellt sich immer wieder die Frage, wie lange die Speicherung von Logfiles erlaubt ist. Explizite gesetzliche Vorgaben dazu gibt es nicht. Der Bundesgerichtshof hat hierzu im Jahr 2014 ein Urteil gefällt, wonach ein Access-Provider im Rahmen der Gewährung der IT-Sicherheit seine Logfiles für eine Dauer von sieben Tagen speichern darf.

Diese äußerst kurze Frist lässt sich auf andere Anbieter wie Websitebetreiber übertragen. Hieraus ergibt sich aber eben auch, dass ein allzu langes Vorhalten von



Ob für die Langzeitarchivierung oder gegen Datenverluste: Ein Backup ist das A und O für jeden, der mit Daten arbeitet. Aber Vorsicht, auch bei dieser „privaten Vorratsdatenspeicherung“ ist rechtlich nicht alles erlaubt.

Logfiles, selbst in Backups, klar gegen den Datenschutz verstößt. Eine Praxis, solche Informationen über Monate zu speichern, ist daher rechtswidrig. Um dieser Problematik zu entgehen, bietet es sich an, in den Logfiles nur gekürzte IP-Adressen zu speichern, die dann nicht mehr als personenbezogen zu betrachten sind.

Ab in die Cloud?

Immer mehr Daten werden in die Cloud exportiert. Dies gilt natürlich auch bei Backup oder Archivierung. Soweit hierfür unternehmenseigene Server zum Einsatz kommen, entstehen aus juristischer Sicht keine Komplikationen. Anders sieht es allerdings aus, wenn Unternehmen personenbezogene Daten an Dienstleister geben und deren Rechner sich außerhalb der EU befinden.

Bei Cloud-Angeboten gilt zunächst einmal die gleiche Regelung wie bei jedem anderen Dienstleister: Werden persönliche Daten an Dritte zum Speichern oder Bearbeiten weitergegeben, ist in aller Regel dafür ein zusätzlicher Vertrag notwendig, eine Vereinbarung zur Auftragsdatenverarbeitung. Darin ist unter anderem zu regeln, wie der Dienstleister mit den Daten zu verfahren hat, wie sie gegen unbefugten Zugriff zu schützen und wann sie wieder zu löschen sind. Zudem muss der Cloud-Anbieter Angaben über seine Maßnahmen zu Datenschutz und vor allem Datensicherheit machen.

Privacy Shield oder Vertrag

Stehen die Rechner des Dienstleisters außerhalb der EU, ist nachzuweisen, dass an dem jeweiligen Ort ein dem hiesigen Standard entsprechendes Datenschutzniveau vorhanden ist. Dies gilt für einige Länder, die als „sichere Drittstaaten“ eingeschätzt werden, etwa die Schweiz, Kanada, Argentinien oder Israel. Insbesondere die USA gehören jedoch nicht dazu. Um den Datentransfer über den Atlantik zu ermöglichen, hat die EU daher ein Abkommen mit den USA geschlossen, den sogenannten Privacy Shield. Wer einen Hoster in den Vereinigten Staaten zur Datenauslagerung nutzt, sollte daher unbedingt darauf achten, dass dieser sich dem Abkommen unterworfen und in die entsprechende Liste auf der Seite privacyshield.gov eingetragen hat. Alternativ dazu kann man eine vertragliche Vereinbarung mit dem Anbieter treffen und dazu die von der EU vorgegebenen sogenannten Standardvertragsklauseln nutzen.

Wann aber müssen gespeicherte Daten zwingend gelöscht werden? Hauptgründe hierfür sind der Wegfall der Rechtsgrundlage oder ein expliziter Löschungswunsch durch den Betroffenen. Fällt der Grund für das Vorhalten der Informationen ersatzlos weg, sind diese zu löschen. Dies gilt beispielsweise nach dem Ende von Vertragsverhältnissen oder wenn das ursprüngliche Angebot eingestellt wird. Auch der Ablauf einer gewissen Zeitspanne kann hier ein Grund sein, beispielsweise am Ende von gesetzlichen Aufbewahrungsfristen.

Das Löschen muss nach dem Wegfall dieser Gründe unverzüglich erfolgen. Selbstverständlich umfasst diese Verpflichtung auch jegliche Form von Backups der erfassten Informationen.

Zudem kann ein Betroffener aktiv das Löschen seiner personenbezogenen Daten verlangen. Auch in diesem Fall hat ein unverzügliches und restloses Entfernen, etwa aus dem CRM, zu erfolgen. Problematisch sind dabei die Fälle, in denen eine Löschungsaufforderung mit gesetzlichen Speicherungspflichten kollidiert. Diesen Konflikt löst Paragraf 35 des BDSG. Er sieht vor, dass in Fällen, in denen einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, die Daten nicht zu löschen, sondern nur zu sperren sind.

Fazit

Die längerfristige Speicherung von Daten ist ein juristischer Drahtseilakt. Auf der einen Seite stehen zwingende gesetzliche Aufbewahrungspflichten neben Anforderungen aus dem Compliance-Bereich. Auf der anderen Seite gebietet der Datenschutz ein möglichst kurzes und streng zweckgebundenes Vorhalten persönlicher Informationen. Um diesen Zielkonflikt zu entschärfen, empfiehlt es sich, entsprechende Speicher- und Löschkonzepte zu entwickeln, die neben den juristischen Vorgaben auch die Interessen aller Beteiligten berücksichtigen. (ur)

Joerg Heidrich

ist Justiziar und Datenschutzbeauftragter von Heise Medien und als Rechtsanwalt in Hannover tätig.

Literatur

[1] Tobias Haar; Recht; Voller Zugriff; Neue Vorgaben für die elektronische Buchführung; *iX* 5/2015, S. 86