Mehr Datenschutz-Skalierung!

Vor der EU-Datenschutz-Grundverordnung DSGVO sind alle (fast) gleich: Es ist egal, ob ein multinationaler Klinikkonzern oder die kleine Naturheilkunde-Praxis medizinische Daten im Internet leakt.

Riesige Konzerne verfügen mit Heerscharen an Security-Experten und Datenschutzanwälten aber über viel mehr Kompetenz und Ressourcen als IT-ferne Kleinunternehmen. Das sind Unterschiede, denen die DSGVO nicht ausreichend Rechnung trägt, wie man aktuell am Fall von Stay Informed (siehe Seite 32) sehen kann: Dieses Unternehmen verwaltet mit seiner App personenbezogene Daten für mehrere Tausend Kitas, Schulen, Pflegeheime und dergleichen. Formal fungiert es als Auftragsverarbeiter, sodass primär eben die Einrichtungen – beziehungsweise deren Träger – für den Datenschutz in der Stay-Informed-App verantwortlich sind.

Man darf bezweifeln, dass sich all diese Einrichtungen ihrer Verantwortung beim Unterzeichnen des Verarbeitungsvertrags bewusst waren. Stay Informed warb sogar mit Aussagen von glücklichen Kunden, die annahmen, sich nun gar nicht mehr um dieses "heikle Thema" kümmern zu müssen. Selbst schuld, könnte man sagen: Eine Kita kann sich nun mal genauso wenig aus der Verantwortung für den Datenschutz stehlen, wie sich ein Restaurant der Verpflichtung zur Nahrungsmittelhygiene entziehen kann.

Das verkennt aber die praktischen Gegebenheiten: Viele, gerade kleinere Einrichtungen haben nicht die Expertise, um Datenschutzrisiken einzuschätzen. Und selbst mit ausreichendem Fachwissen steht und fällt eine Einschätzung damit, ob und wie schnell der Auftragsverarbeiter alle relevanten Informationen zur Verfügung stellt. Vollends absurd ist, dass nun alle betroffenen Kitas und Schulen ein und dasselbe Datenleck an ihre jeweilige Datenschutzaufsicht melden müssen.

Der DSGVO wird viel vorgeworfen, oft zu Unrecht. Aber alle über den gleichen Kamm zu scheren, ist tatsächlich kritikwürdig, egal wie einleuchtend es im Prinzip ist: Es dient dem Datenschutz nicht, wenn verantwortliche Stellen mit ihren Pflichten heillos überfordert sind und Aufsichtsbehörden mit Meldungen überschütten müssen. Der europäische Gesetzgeber sollte den Ansatz "one size fits all" bei der nächsten DSGVO-Evaluierung mindestens hinterfragen.

Sylvester Tremmel

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover