Newsletter Datenschutz

Ausgabe Oktober | 2018

CURACON
SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

Sanovis
Consulting with Care

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

in den vergangenen Wochen kommt das Thema Datenschutz kaum aus den Schlagzeilen. Immer wieder muss Facebook zugeben, dass es zu Pannen und Hackerangriffen gekommen ist. Und nun hat es auch das Pendant Google+ erwischt, mit der Folge, dass der Dienst eingestellt wird.

Aber nicht nur die Weltkonzerne hält das Thema in Atem, auch Mittelständler und Otto-Normal-Verbraucher müssen einige Dinge beachten. So sollten z. B. beim Gebrauch von Cloud-Diensten wichtige Kriterien eingehalten werden und auch bei der Umsetzung der Betroffenenrechte bestehen viele Fragen.

Über diese und weitere Themen rund um den Datenschutz können Sie sich in dieser Ausgabe informieren – wir wünschen Ihnen viel Spaß bei der Lektüre und viele wertvolle Einsichten in den Datenschutz!

Ihr Dr. Uwe Günther, Geschäftsführer, Sanovis GmbH, Geschäftsfeldeiter Datenschutz, Curacon GmbH

Zugriff auf den Account eines Verstorbenen

Facebook ist nur ein Beispiel – die Frage an sich kann sich bei allen sozialen Netzwerken stellen: Was ist, wenn der Inhaber eines Accounts stirbt? Haben seine Erben dann einen Anspruch auf die Daten im Account? Der BGH hat dies in einem Grundsatzurteil bejaht. Er sieht darin keine Verletzung des Datenschutzes.

Der Fall bewegte die Öffentlichkeit sehr, schließlich ging es um ein erst 14-jähriges Mädchen. Sie war unter eine U-Bahn geraten, mit tödlichen Folgen. Die Eltern waren die Erben des Kindes. Außer dem Facebook-Account gab es zwar kaum etwas zu erben. Aber auf den Inhalt des Accounts wollten sie unbedingt zugreifen. Denn sie hofften auf Hinweise, ob der Tod ihrer Tochter ein Selbstmord war.

Sture Haltung von Facebook

Facebook stellte sich freilich quer. Das Unternehmen berief sich auf seine selbst gemachten Regeln: Da irgendwer Facebook den Tod des Mädchens mitgeteilt hatte, wurde der Account in einen „Gedenkzustand" versetzt. Nur die beim Tod schon vorhandenen „Freunde" konnten die Einträge sehen und Erinnerungen hinterlassen. Von einem Zugriff durch Erben wollte Facebook nichts wissen.

Der BHG gewährt den Zugriff

Um ihr Ziel zu erreichen, mussten die Eltern durch drei Instanzen klagen. Beim Bundesgerichtshof (BGH) bekamen sie schließlich auf der ganzen Linie Recht. Er verurteilte Facebook dazu, den Eltern als Erben Zugriff auf die Daten im Account zu geben.

Erbrecht als Ausgangspunkt

Die Hauptargumente des BGH zum Erbrecht lauten so:

- Bei einem Erbfall geht das gesamte Vermögen des Verstorbenen auf die Erben über. Zum Vermögen in diesem Sinn gehören auch Vertragsbeziehungen. Die Eltern haben also gewissermaßen den Vertrag ihrer Tochter mit Facebook geerbt. Damit haben sie das Recht, auf den Inhalt des Accounts zuzugreifen. Im Ergebnis ist das nichts anderes, als wenn sie ein Tagebuch oder Briefe geerbt hätten, die ihrer Tochter gehörten.

- Facebook darf diese Rechtslage nicht dadurch unterlaufen, dass es einen „Gedenkzustand" erfindet und den Zugriff blockiert. Denn im Vertrag zur Nutzung von Facebook steht davon nichts.

Datenschutz kein Hindernis

Kein Problem sieht der BGH im Datenschutz. Dabei unterscheidet er so:

- Für das verstorbene Mädchen gelten die Datenschutz-Regelungen nicht mehr. Die Datenschutz-Grundverordnung (DSGVO) bezieht sich ausdrücklich nur auf lebende Personen. Auf Daten Verstorbener ist sie nicht anzuwenden.

- Die Kommunikationspartner des Mädchens, die Einträge auf Facebook hinterlassen haben, können sich zwar prinzipiell auf die DSGVO berufen. Zu Lebzeiten des Mädchens war die Verarbeitung dieser Daten jedoch erforderlich, weil die Kommunikation über den Account sonst nicht funktioniert hätte. Damit war die Verarbeitung berechtigt. Der Tod des Mädchens ändert daran nichts. Die Verarbeitung der Daten durch Facebook bleibt weiterhin rechtmäßig. Die Erben des Mädchens nehmen nur die Möglichkeit zum Datenabruf wahr, die das Mädchen zu Lebzeiten selbst hatte.

Noch zwei kurze Hinweise

Wichtig ist bei diesen Überlegungen, dass sie generell für alle Erben gelten. Keine Rolle spielt, dass die Erben des Mädchens zugleich ihre Eltern waren und das Sorgerecht besaßen.

Mit dem Aktenzeichen III ZR 183/17 ist das Urteil im Internet leicht zu finden.

Auskunftsrecht nach der DSGVO

Die DSGVO gibt Personen, deren Daten irgendwo gespeichert sind, viele Rechte. Am wichtigsten ist dabei das „Auskunftsrecht der betroffenen Person". Wer es ausüben will, muss einige Spielregeln kennen. Der interne Aufwand für Unternehmen kann auch bei korrekten Anfragen enorm sein. Die DSGVO nimmt darauf letztlich keinerlei Rücksicht. Ob ein Antragsteller mit der Antwort inhaltlich etwas anfangen kann, ist wiederum sein Problem.

Auskunftsrecht als „Recht der Rechte"

Das Auskunftsrecht gilt als das wichtigste Recht, das die DSGVO gewährt. Ein wesentlicher Grund dafür: Nur wer weiß, wo Daten über ihn gespeichert sind, kann weitere Rechte geltend machen, etwa das Recht auf die Berichtigung von falschen Daten.

Zwei Stufen des Rechts

Genau genommen unterscheidet die DSGVO in ihrem Artikel 15 zwei Stufen des Auskunftsrechts:

- **Stufe 1:** Die betroffene Person kann Auskunft darüber verlangen, ob ein Unternehmen oder eine Behörde überhaupt über Daten verfügt, die sie betreffen. Die Antwort auf diese Frage ist im Ergebnis einfach: Ist das der Fall, lautet die Antwort „ja" (Fall der Positivauskunft). Ist das nicht der Fall, lautet die Antwort „nein" (Fall der Negativauskunft).

- **Stufe 2:** Falls Daten vorhanden sind, besteht ein Anspruch der betroffenen Person, diese Daten zu erhalten. Außerdem muss sie eine ganze Reihe von Informationen zu den Daten bekommen. Dazu gehört etwa die Angabe des Zwecks, zu dem die Daten verarbeitet werden.

Berechtigte Sorge der Unternehmen vor dem Aufwand

Das umfassende Auskunftsrecht ist sicher eine große Errungenschaft des Datenschutzrechts. Dennoch sind viele Unternehmen davon nicht nur begeistert. Sie haben keineswegs etwas zu verbergen, wie manche Kritiker glauben. Vielmehr fürchten sie den Aufwand, den solche Anfragen verursachen. Er ergibt sich aus mehreren Aspekten:

- Zunächst einmal muss überall im Unternehmen gesucht werden, ob Daten über die anfragende Person vorhanden sind. Hinweise darauf, wo wahrscheinlich etwas zu finden ist, erleichtern die Suche. Beispiel: Die anfragende Person gibt an, dass sie mehrfach als Zeitarbeiter im Unternehmen gearbeitet hat. Ausdrücklich verpflichtet ist sie zu solchen Angaben allerdings nicht. Sinnvoll sind sie trotzdem. Sie können eine Antwort wesentlich beschleunigen.

- Der Auskunftsanspruch betrifft auch Daten auf Papier. Dies kann den Aufwand bei der Suche vervielfachen. Die DSGVO nimmt auf die Besonderheiten von Daten auf Papier letztlich keine Rücksicht mehr.

- Der Auskunftsanspruch ist zeitlich nicht begrenzt. Er erstreckt sich auf alle Daten, die vorhanden sind – auch auf solche, die schon viele Jahre unangetastet im Firmenkeller liegen.

- Der Auskunftsanspruch besteht auch dann, wenn es um sehr große Datenmengen geht, etwa um mehrere tausend Seiten.

Recht auf eine kostenlose Kopie

Sind die Daten gefunden, hat die anfragende Person Anspruch auf eine kostenlose Kopie. Besonders bei umfangreichen Papierunterlagen kann dies für das Unternehmen ins Geld gehen. „Eine" Kopie ist dabei wörtlich zu nehmen. Wer eine zweite Kopie will, etwa weil er die erste Kopie verloren hat, muss dafür zahlen

Notwendige Vernichtungsaktionen

Viele Firmen haben die DSGVO zum Anlass genommen, entbehrliche Unterlagen zu vernichten. Solche Aktionen sind bei Mitarbeitern nicht immer beliebt, aber wichtig. Wenn die gesetzlichen Aufbewahrungsfristen (beispielsweise aus dem Steuerrecht) abgelaufen sind, steht einer Vernichtung von Unterlagen nichts entgegen.

Grenzen bei Geschäftsgeheimnissen

Der Auskunftsanspruch geht zwar weit. Grenzen hat er aber trotzdem. So ist ausdrücklich festgelegt, dass „das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen" darf. Dies wirkt abstrakt, hat aber sehr konkrete Auswirkungen. In den Erwägungsgründen der DSGVO ist als Beispiel genannt, dass der Auskunftsanspruch Geschäftsgeheimnisse nicht beeinträchtigen darf. Der Auskunftsanspruch darf sie also nicht aushebeln.

Kein Anspruch auf eine verständliche Auskunft

Wer Auskunft verlangt, erhält die Daten übrigens so, wie sie vorliegen. Ob er inhaltlich mit ihnen etwas anfangen kann, ist sein Problem. Denn einen Anspruch auf Erläuterung des Inhalts von Daten sieht die DSGVO nicht vor. Dies wird vor allem im Bereich der Medizin wichtig. In der DSGVO heißt es ausdrücklich, dass sich der Auskunftsanspruch auch auf Daten in Patientenakten bezieht. Die Verständlichkeit der dort verwendeten Fachbegriffe und Kürzel ist damit in keiner Weise garantiert. Es ist Sache des Antragstellers, wie er damit klarkommt.

Einmal-Passwörter per SMS: Sind sie wirklich sicher?

Ein Passwort allein reicht als Schutz vor unberechtigtem Zugang zu IT-Systemen oftmals nicht aus. Deshalb nutzen viele Online-Dienste zusätzlich Einmal-Passwörter, die sie per SMS an den Nutzer schicken und die als zweiter Sicher-heitsfaktor dienen. Doch wie sicher ist das?

Zugangsdaten werden gestohlen oder geknackt

Stellen Sie sich vor, ein Freund teilt Ihnen mit, dass er eine Spam-Mail von Ihnen bekommen hat. Entweder jemand benutzt Ihren Namen für Spam, oder Ihr Web-Mail-Konto wurde missbraucht. Sie versuchen, sich bei Ihrem Web-Mail-Zugang anzumelden, doch Ihr Passwort wird nicht mehr akzeptiert. Der Grund: Ihr Mail-Provider hat den Spam-Versand von Ihrem Web-Mail-Konto festgestellt und Ihr Konto deshalb sicherheitshalber deaktiviert.

Wie konnte das geschehen? Offensichtlich hatte ein Spammer Ihr Mail-Passwort. Es war ungeschützt gespeichert, oder Sie haben es eingegeben, während Ihre Tastatur-eingaben mitgeschnitten wurden. Oder aber Ihr Passwort war so einfach, dass ein Angreifer es schlicht erraten und geknackt hat.

Zusätzliche Sicherheitsfaktoren sollen davor schützen

Um das zu vermeiden, setzen immer mehr Online-Dienste auf eine sogenannte Zwei-Faktor-Authentifizierung. Dabei reicht ein Passwort zur Anmeldung nicht aus. Es gibt einen zweiten Sicherheitsfaktor, der ebenfalls für die Anmeldung benötigt wird. Meist ist dies ein sogenanntes Einmal-Passwort, ein für Sie generiertes zweites Passwort, das nur ein einziges Mal gilt.

Dieses Einmal-Passwort wird an den Nutzer meistens per SMS geschickt. Im Online-Banking wird dabei gefordert, dass das Smartphone, mit dem das Banking gemacht wird, nicht das gleiche Gerät sein darf, an das das Einmal-Passwort per SMS gesendet wird, aus Sicherheitsgründen. Doch wie sicher sind Einmal-Passwörter per SMS überhaupt?

Ungeschützte SMS sind ein Risiko

In der Regel liegen Nachrichten, die per SMS eingetroffen sind, unverschlüsselt auf dem Smartphone oder Handy. Eine Verschlüsselung findet man nur dann, wenn man die Nachrichten-App oder die SMS-App in einem geschützten Bereich auf dem Smartphone betreibt. Zudem muss man sich klarmachen, dass viele Apps bei ihrer Installation oder im Rahmen eines App-Updates die Berechtigung verlangen, SMS zu lesen.

Nicht jede App, die auf SMS zugreifen will, braucht diese Berechtigung, im Gegenteil. Zudem gibt es bösartige Apps, die die SMS auslesen und den Inhalt missbrauchen könnten, zum Beispiel um einen starken Zugangsschutz zu umgehen, bestehend aus Nutzer-Passwort und Einmal-Passwort, das per SMS eingetroffen ist

Angriffe auf starken Zugangsschutz waren bereits erfolgreich

Berichte über Vorfälle in dieser Art (etwa der sogenannte Reddit-Hack) zeigen, dass man nicht ohne Weiteres annehmen kann, dass die SMS, mit der das Einmal-Passwort geschickt wird, sich nicht ausspähen lässt. Neben dem Nutzer-Passwort könnte also auch das Einmal-Passwort, das per SMS kommt, in unbefugte Hände geraten.

Was ist genau beim Reddit-Hack passiert? Darüber hat zum Beispiel der IT-Sicherheitsanbieter 8com berichtet. Das Unternehmen Reddit setzt für seine Mitarbeiter auf eine Zwei-Faktor-Authentifizierung. Trotzdem konnten Mitte Juni Hacker in die Datenbanken von Reddit eindringen und Nutzerdaten erbeuten. Um sich Zugang zu den internen Netzwerken zu verschaffen, mussten die Kriminellen sowohl das Passwort als auch das Einmal-Passwort in der SMS des jeweiligen

Mitarbeiters eingeben. Die SMS erhielten sie, indem sie sich eine Kopie der SIM-Karte des Mitarbeiters mit derselben Nummer beschafften. So konnten sie die SMS abfangen.

An eine Kopie einer SIM-Karte zu gelangen, ist nicht so kompliziert, wie man denkt, berichtet 8com. Manchmal reicht schon ein Anruf beim Anbieter, dass die SIM-Karte kaputt sei und man eine neue brauche. Zwar muss man sich dann legitimieren, aber viele Menschen geben die dafür relevanten Informationen wie den Geburtstag ganz öffentlich im Internet preis.

Trotzdem: Zwei-Faktor-Authentifizierung bleibt wichtig

Bedeuten Vorfälle wie der Reddit-Hack, dass ein starker Zugangsschutz gar nicht stark ist? Sicherheitsexperten sagen, dass es in jedem Fall besser ist, ein Einmal-Passwort zusätzlich einzusetzen, als nur ein einzelnes Passwort. Doch man sollte lieber zu anderen Methoden übergehen, um Einmal-Passwörter zu erzeugen, etwa zu Security-Token.

Security-Token sind spezielle Geräte, um Einmal-Passwörter zu erzeugen. Sie haben im Vergleich zu Smartphones einige Vorteile. Unter anderem installiert der Nutzer auf Security-Tokens keine fremden Apps, die die Erlaubnis bekommen, SMS-Nachrichten zu lesen, und dies missbrauchen könnten. Zudem brauchen Security-To keine SIM-Karten, die Datendiebe „nachbestellen" könnten.

Impressum

Redaktion:
Dr. Uwe Günther
Sanovis GmbH

Anschrift:
Richard-Strauss-Str. 69
81679 München
Telefon: +49 89 99 27 579 22
E-Mail: Uwe.Guenther@Sanovis.com

Wie lassen sich neue Anwendungen datenschutzgerecht testen?

Ständig kommen neue Cloud-Dienste auf den Markt. Doch leisten sie, was sie versprechen? Wenn Sie dies testen wollen, denken Sie auch an den Datenschutz, bevor Sie zum Beispiel Kundendaten testweise in eine Cloud übertragen.

Die Cloud gehört zum Firmenalltag

Im Jahr 2017 nutzten zwei Drittel aller Unternehmen (66 Prozent) Rechenleistungen aus der Cloud, so eine Umfrage des Digitalverbands Bitkom. Wer Cloud-Anwendungen nutzt oder damit plant, für den ist Datenschutz das Top-Kriterium, wenn es um die Auswahl eines Cloud-Dienstleisters geht. Praktisch alle Unternehmen (97 Prozent) gaben an, dass für sie die Konformität mit der Datenschutz-Grundverordnung (DSGVO) bei Cloud-Lösungen unverzichtbar ist.

In der Vergangenheit beklagten jedoch viele Unternehmen Ausfälle der Cloud-Lösungen. Insgesamt konnten sieben von zehn Cloud-Anwendern (69 Prozent) kurzzeitig nicht auf ihre Cloud-Dienste zugreifen. Dafür gibt es verschiedene Ursachen: Am häufigsten waren technische Probleme aufseiten des Cloud-Providers (46 Prozent) dafür verantwortlich.

Es ist deshalb auch aus Datenschutzsicht mehr als sinnvoll, nicht nur auf dem Papier zu prüfen, ob ein Cloud-Dienst sicher und zuverlässig ist.

Erst testen, dann nutzen

Es sollte selbstverständlich sein, einen neuen Cloud-Dienst ausgiebig zu testen, um zu sehen, ob er die fachlichen und technischen Anforderungen erfüllt. Auch die Datenschutzfunktionen einer Cloud-Lösung gehören auf den Prüfstand, bevor der Dienst zum Einsatz kommt.

Selbst wenn es Gütesiegel sowie Datenschutz- und IT-Sicherheitszertifikate gibt, bleibt insbesondere die Frage, ob die fachlichen Anforderungen des Nutzers, der Abteilung oder allgemein des Unternehmens erfüllt werden können. Um das zu überprüfen, sind in der Regel Testdaten erforderlich.

Achtung: Ein Test ist bereits der Ernstfall

Die Aufsichtsbehörden für den Datenschutz weisen bereits seit vielen Jahren darauf hin, dass der Testfall für den Datenschutz bereits der Ernstfall ist. Deshalb kommt es auf die richtige Vorbereitung der Testdaten an. Ein denkbarer Schutz für die Testdaten mit Personenbezug wäre die Verschlüsselung. Doch vielfach werden die Daten nicht verschlüsselt, weil die zu testende Cloud-Lösung nicht mit den verschlüsselten Daten umgehen kann.

Deshalb sind Verschlüsselungslösungen sinnvoll und hilfreich, die aus den Echtdaten sogenannte Tokens erzeugen. Bei der Tokenisierung werden die zu schützenden, vertraulichen Daten durch Daten desselben Typs, also passender Art und Länge ersetzt. Die neuen Werte (Tokens) weisen aber keinen echten Personenbezug mehr auf.

Datenschutzniveau muss stimmen

Dadurch simulieren die entsprechend veränderten Daten die Nutzung echter Daten, ohne jedoch den Datenschutz zu gefährden. Fachliche Tests der Funktionen einer Cloud-Lösung werden so möglich, ohne personenbezogene Daten zum Test in eine Cloud zu übertragen. Nicht nur bei Cloud-Diensten, die jenseits der EU betrieben werden, könnte dies sonst zum Datenschutzproblem werden, sondern generell muss sichergestellt sein, dass das Datenschutzniveau der Cloud-Lösung den Vorgaben der DSGVO entspricht.

Wichtig ist es dabei, nicht einfach eine Lösung dafür zu nutzen, die der Anbieter, den man testen möchte, bereitstellt. Oftmals lässt sich dann nicht ausschließen, dass Mitarbeiter des Anbieters die Testdaten unerlaubt wieder zugänglich machen könnten. Die Verschlüsselung und die Tokenisierung sollten immer in der Hoheit des Nutzers liegen, die Schlüssel sollten also beim Anwender vorgehalten werden, auch schon im Testfall.

Denken Sie beim Test an den Datenschutz?

Frage: ***Wird eine Cloud-Lösung lediglich getestet, muss es kein Datenschutzkonzept dafür geben. Stimmt das?***

a. **Nein, nicht nur im Produktivfall muss der Datenschutz stimmen, auch bereits im Testfall.**

b. **Ja, denn beim Testen werden ja nur Testdaten genutzt.**

Lösung: Die Antwort a. ist richtig. Bereits im Testfall muss der Datenschutz beachtet werden. Zudem nutzen viele Unternehmen als Testdaten ihre echten Produktivdaten. Denn der Test soll ja realistisch sein, so denken sie. In Wirklichkeit vergessen sie dabei den Datenschutz, wenn sie die Testdaten nicht richtig aufbereiten.

Frage: ***Testdaten ohne Personenbezug sind unrealistisch und machen Tests wertlos. Stimmt das?***

a. **Ja, denn eine Lösung zur Kundendatenverwaltung muss mit Kundendaten getestet werden.**

b. **Nein, Sind die Testdaten richtig aufbereitet und von ihrem Personenbezug befreit, bleiben sie fachlich korrekte Daten für den Test.**

Lösung: Hier ist die Antwort b. richtig. Mit dem richtigen Verfahren behalten die Testdaten die Struktur und Länge, die sie fachlich brauchen. Ein solches Verfahren ist die sogenannte Tokenisierung. Wie oben erläutert, werden bei der Tokenisierung die zu schützenden vertraulichen Daten durch Daten desselben Typs, also passender Art und Länge ersetzt. Die neuen Werte (Tokens) weisen aber keinen echten Personenbezug mehr auf. Der Datenschutz lässt sich so auch im Testfall wahren und verhindert keinen Test.