Newsletter Datenschutz

Ausgabe Dezember | 2018

CURACON
SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

Sanovis
Consulting with Care

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

die Datenschutz-Grundverordnung (DSGVO) hat das Interesse an Fragen rund um den Datenschutz deutlich erhöht. Doch es herrscht einiges an Unklarheit und Verwirrung, Aufklärung tut not. Genau hier setzt Ihre neue Datenschutz-Zeitung an. So erfahren Sie, was es wirklich mit den gefürchteten Geldbußen auf sich hat, die bei einer Datenschutzverletzung verhängt werden können. Ebenso finden Sie in dieser Ausgabe wichtige Hinweise, was bei Bildern von Personen aus Sicht des Datenschutzes zu beachten ist.

Andere Themen wie das Löschen von Daten aus einem Cloud-Dienst werden weniger stark diskutiert, erfordern aber deutlich mehr Aufmerksamkeit. Das Datenlöschen ist deshalb ebenso in dieser Ausgabe zu finden wie die meist unbekannte Gefahr durch sogenannte Webroboter, die Daten im Internet sammeln und missbrauchen.

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

Ihr Stefan Strüwe, Senior Manager, Geschäftsfeld Datenschutz, Curacon GmbH

Geldbußen nach der DSGVO

Der Begriff „Geldbuße" klingt so, als ginge es um ein paar Euro. Bei den Geldbußen nach der Datenschutz-Grundverordnung (DSGVO) sieht das allerdings etwas anders aus. Und auch sonst weisen sie einige Besonderheiten auf, die man kennen sollte.

Geldbußen in maßloser Höhe?

„Irrsinn" war ein Begriff, den man anfangs häufig hören konnte, wenn es um die mögliche Höhe von Geldbußen nach der DSGVO ging. Und tatsächlich: Eine maximale Höhe von 20 Millionen Euro ist eine echte Ansage. Doch wie so oft im Leben sollte man auch hier genauer hinsehen, um was es eigentlich geht.

Die DSGVO gilt für Kleinstunternehmen genauso wie für Großkonzerne. Das muss sich in der möglichen Höhe von Geldbußen widerspiegeln. Deshalb ist es konsequent, wenn die DSGVO in ihrem Art. 83 Abs. 6 von „bis zu" 20 Millionen Euro Geldbuße spricht. Geringfügige, einmalige Verstöße in kleinen Unternehmen werden also nur überschaubare Beträge kosten. Auf Dauer angelegte, bewusste Verstöße in Großunternehmen können dagegen teuer werden. Diese Unterscheidung entspricht dem Prinzip der Verhältnismäßigkeit.

Wer ist „Verantwortlicher"?

Geldbußen sind nur gegen „Verantwortliche" möglich. Der Begriff legt nahe, dass bei einem Verstoß in einem Unternehmen zunächst der intern Verantwortliche gesucht wird und dass ihn dann die Geldbuße trifft. Doch weit gefehlt: Die DSGVO definiert den Begriff „Verantwortlicher" in ihrem Art. 4 Nr. 7 ganz anders: „Verantwortlicher" ist das Unternehmen selbst, nicht der Mitarbeiter! Geldbußen gegen einzelne Mitarbeiter sieht die DSGVO nicht vor.

Kein Freibrief für pflichtvergessene Mitarbeiter!

Eine gute Nachricht für Mitarbeiter, die es mit dem Datenschutz nicht so genau nehmen? Nicht wirklich. Denn eine Geldbuße für ihre Pflichtverletzung wird dann logischerweise gegen das Unternehmen verhängt. Als Folge für die Mitarbeiter selbst stehen Abmahnungen oder sogar ernstere arbeitsrechtliche Schritte im Raum. Das wiegt mindestens genauso schwer wie eine Geldbuße.

Der „Freischuss" – ein rechtliches Märchen!

Immer wieder macht das Gerücht die Runde, dass die Datenschutz-Aufsichtsbehörden bei erstmaligen Verstößen sehr nachsichtig seien. Manche sprechen sogar von einem angeblichen „Freischuss", der jedem Unternehmen zustehe.

Bei näherem Hinsehen stimmt an diesem Gerücht schlicht nichts. Natürlich kann es vorkommen, dass ein leichter, lediglich fahrlässiger Verstoß gegen Vorschriften nur zu einer Ermahnung führt. Das kennt jeder schon von Verkehrsverstößen. Aber wenn der Verstoß gravierend ist, scheidet eine solche Nachsicht aus. Dann kann auch schon ein erstmaliger Verstoß eine Geldbuße in beträchtlicher Höhe nach sich ziehen.

Aufrüstung der Aufsichtsbehörden

Manche fragen sich, warum man von solchen Fällen fast nie hört. Der Grund ist einfach: Auch die Aufsichtsbehörden für den Datenschutz müssen sich erst auf die neuen Regelungen der DSGVO einstellen. Zudem müssen sie neues Personal anlernen. Aber in einigen Monaten sieht das schon anders aus. Und dann besteht ein echtes Risiko von Geldbußen.

Bilder und Datenschutz

Angeblich bringt die Datenschutz-Grundverordnung (DSGVO) völlig neue Regelungen für den Umgang mit Bildern von Personen. Dichtung und Wahrheit liegen bei dieser Behauptung nahe beieinander.

Ein spektakulärer Fall: Erinnerungsfotos im Kindergarten

Der Fall löste Fassungslosigkeit aus: In Berlin machte ein Kindergarten Erinnerungsfotos mit allen Kindern, die in die Grundschule wechselten. Doch die Freude von Kindern und Eltern über die Fotos war deutlich getrübt. Denn die Gesichter der Kinder waren entweder verpixelt oder mit „schwarzen Balken" über den Augen versehen. Die Begründung des Kindergartens: Die DSGVO verlangt das leider so!

Diese Aussage war allerdings Unfug. Dass die Kinder fotografiert werden, war angekündigt, und die Eltern waren damit ersichtlich einverstanden. Zudem wurden die Bilder nur den beteiligten Kindern und Eltern ausgehändigt. Also im Ergebnis alles kein Problem. Der Fall zeigt jedoch deutlich, wie groß die Unsicherheit beim Thema „Bilder und DSGVO" inzwischen ist.

Keine Spezialregelungen in der DSGVO

Wer den Text der DSGVO zur Hand nimmt, erlebt eine Überraschung: Für Abbildungen von Personen finden sich keinerlei spezielle Regelungen! Allerdings gilt natürlich: Wenn Personen auf einem Bild zu identifizieren sind, dann enthält dieses Bild personenbezogene Daten. Dies hat der Europäische Gerichtshof sogar schon ausdrücklich festgehalten und das so formuliert: „Das von einer Kamera aufgezeichnete Bild einer Person fällt unter den Begriff der personenbezogenen Daten."

Rein private Fotografien

Vom Prinzip her ist die DSGVO somit auf Abbildungen von Personen anwendbar. Freilich gibt es davon eine wichtige Ausnahme. Sie betrifft den Fall, dass Bilder im rein persönlichen oder im rein familiären Rahmen entstehen. Wer also seine Kinder am Strand fotografiert oder seine Freundin neben dem Weihnachtsbaum, muss sich dabei nicht um Vorgaben der DSGVO kümmern.

Kommerzielle Verwendung von Fotos

Das ändert sich jedoch, wenn privat entstandene Bilder kommerziell verwendet werden. Hier ein klassisches Beispiel: Ein Mann betreibt einen Ponyhof. Er fotografiert seine elfjährige Tochter auf einem Pony. Solange er dieses Bild im privaten Bereich belässt, findet die Datenschutz-Grundverordnung keine Anwendung. Stellt er das Bild dagegen auf die Homepage des Ponyhofs, hat er den rein privaten Bereich verlassen, und die DSGVO ist anwendbar.

Ein echter Fall

Der Fall hat sich tatsächlich so ereignet. Die Eltern des Kindes lebten getrennt, hatten aber die gemeinsame elterliche Sorge. Die Mutter hatte etwas dagegen, dass die Tochter auf der Homepage des Ponyhofs erscheint. Sie konnte einen entsprechenden Unterlassungsanspruch durchsetzen. Das lag vor allem daran, dass sie als Mit-Sorgeberechtigte übergangen worden war.

Das Bild im Zutrittsausweis

Nichts wirklich Neues bringt die DSGVO für Bilder im Arbeitsleben. Das klassische Beispiel: In einem Industriebetrieb wird für jeden Beschäftigten ein Zutrittsausweis mit Bild ausgestellt. Das soll sicherstellen, dass sich Unbefugte keinen Zutritt zum Gelände verschaffen können. Das Anfertigen eines Bilds und seine Anbringung im Ausweis sind in diesem Fall erforderlich, um das Arbeitsverhältnis ordnungsgemäß durchführen zu können. Damit ist dieses Vorgehen erlaubt. So war es schon bisher, und so ist es auch künftig. Das steht jetzt nur an anderer Stelle im Gesetz, nämlich in § 26 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG).

Gruppenfotos von Arbeitsjubilaren

Anders sieht es dagegen aus, wenn zum Beispiel ein Gruppenfoto von Arbeitsjubilaren angefertigt werden soll. Dies ist für das Beschäftigungsverhältnis nicht erforderlich. Daher ist die Einwilligung jedes einzelnen nötig, der auf dem Foto zu sehen sein soll. Diese Einwilligung bedarf sogar der Schriftform, wenn nicht ganz besondere Umstände vorliegen (§ 26 Abs. 2 Satz 3 BDSG). Der deutsche Gesetzgeber hat damit für Einwilligungen im Arbeitsleben eine Schriftform eingeführt, die in der DSGVO nicht vorgesehen ist. Er durfte dies tun, weil die DSGVO den Gesetzgebern der Mitgliedstaaten erlaubt, für das Arbeitsleben besondere Datenschutzregelungen einzuführen.

Einwilligungslisten

Ob die Sache mit der Schriftform eine gute Idee war, darüber kann man freilich geteilter Meinung sein. Einen Vorteil hat die Schriftform jedenfalls: Es ist klar dokumentiert, wer einverstanden war. Dabei ist es übrigens kein Problem, wenn eine Liste verwendet wird, auf der alle unterschreiben. Oben auf der Liste muss lediglich stehen, um was es geht. Dazu gehören vor allem der Anlass („Fotos von Arbeitsjubilaren") und Angaben dazu, wo die Bilder veröffentlicht werden sollen (Beispiel: „In der Firmenzeitschrift und im Firmennetz"), müssen dort genannt sein.

Eines zeigen alle Beispiele sehr deutlich: Wer mit gesundem Menschenverstand vorgeht, wird bei Bildern kaum in Konflikt mit der DSGVO geraten.

Automatisierter Datenmissbrauch: Angriff der Webroboter

Wenn das tolle Online-Angebot sofort ausgebucht ist, müssen nicht andere Kunden schneller gewesen sein als Sie. Webroboter oder Bots erobern das Internet, kaufen komplette Angebotsbestände auf und verkaufen sie woanders zu einem höheren Preis. Womöglich missbrauchen sie dabei sogar Ihre Kreditkartendaten.

Schon wieder ein Captcha-Test...

Sie sitzen vor dem PC und wollen sich bei einem Online-Portal anmelden. Für das Log-in reicht es aber nicht, dass Sie Benutzername und Passwort eingeben, Sie sollen auch noch eine Art Bilderrätsel lösen. Sie werden zum Beispiel aufgefordert, alle Bildchen anzuklicken, die ein Straßenschild zeigen. Im nächsten Schritt bekommen Sie noch eine weitere Bilder-Aufgabe, langsam werden Sie ungeduldig, vielleicht verzweifeln Sie fast, weil Sie scheinbar ein passendes Bildchen übersehen haben und nicht weiterkommen.

Doch diese sogenannten Captcha-Tests haben ihren Sinn. Sie sollen nicht etwa Ihre genaue Identität überprüfen, wie es eine Zwei-Faktor-Anmeldung macht, bei der zum Beispiel ein Einmal-Passwort per SMS kommt. Captcha-Tests sollen nur prüfen, ob Sie ein Mensch sind oder ob doch eine Maschine hinter der Anmeldung steckt. Tatsächlich sind sehr viele Webroboter oder Bots im Internet unterwegs, also Softwareautomaten, die mit Webseiten und Online-Diensten interagieren.

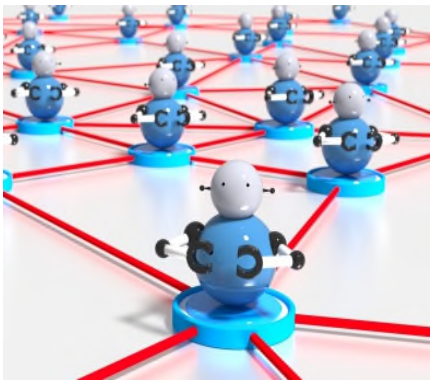
Bots machen bereits die Hälfte des Internetverkehrs aus

Internetdienstleister, die den weltweiten Datenverkehr beobachten, berichten davon, dass die Webroboter bereits für jede zweite Online-Verbindung verantwortlich sind. Bei der großen Zahl an Webroboter-Aktivitäten ist es also kein Wunder, dass Online-Dienste wissen wollen, ob es ein Bot oder ein Mensch ist, der sich für ihr Angebot anmelden will. Webroboter sind nämlich nicht immer harmlos, ganz im Gegenteil.

Internetkriminelle setzen Webroboter ein, um zum Beispiel Online-Werbung anzuklicken. Die Werbekunden glauben dann, ihre Online-Werbung hätte großes Interesse erzeugt, und müssen deutlich mehr bezahlen, als der Werbeerfolg in Wirklichkeit wert ist. Oder die Bots überfallen Online-Shops, überlasten sie und bringen den Webserver des Shop-Betreibers zum Absturz.

Die Webroboter können aber auch bestellen und Online-Aktionen ausnutzen, um günstig an Ware zu kommen, die dann teurer verkauft wird. Nicht zuletzt durchsuchen sie das Netz nach personenbezogenen Daten, die sie danach missbrauchen. Die Folge sind Spam-Attacken oder der Diebstahl von ungeschützten Kreditkartendaten.

Online-Provider und Online-Nutzer müssen sich schützen



Damit Online-Dienste, aber auch Internetnutzer gegen Webroboter geschützt sind, müssen Bots erkannt und abgewehrt werden. Dazu dienen die erwähnten Captcha-Tests. Doch das allein reicht nicht als Gegenmaßnahme. Denn es gibt auch gutartige Webroboter, die man nicht blockieren will. Ein Beispiel sind Webroboter, die Suchmaschinen und andere Informationsdienste einsetzen, um zum Beispiel einen Online-Shop in ein Branchenverzeichnis aufzunehmen.

Damit man nicht die gutartigen Bots und damit die falschen abwehrt, müssen also Lösungen zum Einsatz kommen, die sowohl Menschen und Webroboter als auch dann noch die Art des Webroboters unterscheiden können. Unternehmen, die Online-Dienste anbieten, sollten sich mit solchen Lösungen befassen.

So arbeitet eine Bot-Erkennung und –Abwehr

Meist setzen Unternehmen Lösungen ein, die als Bot-Manager bezeichnet werden. Sie klassifizieren die Webroboter und können sie von Menschen unterscheiden. Und zwar mithilfe von Verfahren, die das Online-Verhalten analysieren. Gute Anbieter nutzen dabei nur solche Methoden, die den Menschen als Nutzer anonymisieren.

Bot-Manager werten sowohl das Tippverhalten als auch die Mausbewegung bei Desktop-Nutzern. Sie untersuchen mobile Zugriffe daraufhin, wie die Interaktion mit der jeweiligen App aussieht, wie der Nutzer das mobile Endgerät hält oder wie die Berührung des Touchscreens abläuft. Menschen und Bots zeigen hier Unterschiede, selbst bei aufwendig entwickelten Bots. Hat der Bot-Manager einen Webroboter erkannt, findet noch ein Abgleich mit einer Datenbank statt, die die gutartigen Bots listet.

Wichtig: Datenminimierung und Verschlüsselung!

Was aber kann man als normaler Internetnutzer tun, denn die Bot-Manager unterstützen ja die Online-Anbieter? Wichtig ist es für Sie als Online-Nutzer, dass Sie wissen, dass es im Internet Webroboter gibt, die Ihre Daten blitzschnell einsammeln können und dann womöglich nutzen, um bei der nächsten Online-Aktion alle Angebote aufzukaufen, vielleicht sogar auf Ihre Rechnung.

Denken Sie deshalb im Internet an die Datenminimierung, seien Sie sparsam mit persönlichen Angaben und verschlüsseln Sie Ihre Daten. Dann haben Webroboter, die Internetkriminelle einsetzen, keine Chance gegen Sie!

Impressum

Redaktion
Dr. Uwe Günther
Sanovis GmbH

Stefan Strüwe, RA
CURACON GmbH
Wirtschaftsprüfungsgesellschaft

Anschrift
Richard-Strauss-Str. 69
81679 München
Telefon: 089 / 99 27 579 22
E-Mail: Uwe.Guenther@Sanovis.com

Am Mittelhafen 14
48155 Münster
Telefon: 02 51 / 92 208 209
E-Mail: Stefan.Struewe@curacon.de

Datenlöschen in der Cloud: Was wirklich nach dem Löschen passiert

Wer seine Daten aus einem Online-Speicherdienst löschen möchte, muss scheinbar nur den richtigen Browser-Knopf drücken. Doch sind die Daten dann sofort gelöscht? Google hat nun das Löschverfahren für die Google Cloud beschrieben.

Cloud-Dienste und der Datenschutz

Zwei von drei Unternehmen in Deutschland nutzen bereits Cloud Computing, also IT-Dienste wie Speicherplatz, Rechenleistung und Anwendungen aus dem Internet. Wie der Cloud Monitor 2018 des Digitalverbands Bitkom ergab, sind die Unternehmen bei der Wahl des Cloud-Dienstes zu Recht darauf bedacht, dass sie die Datenschutz-Grundverordnung (DSGVO) einhalten.

Die DSGVO fordert unter anderem, dass personenbezogene Daten von Kunden unter bestimmten Voraussetzungen unverzüglich zu löschen sind. Das gilt zum Beispiel dann, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind und keine Aufbewahrungspflichten etwa steuerlicher Art bestehen.

Die Löschpflicht betrifft nicht nur das interne Netzwerk und die Computer, die Ihr Unternehmen selbst betreibt, sondern auch die personenbezogenen Daten, die in einer Cloud gespeichert sind. Doch wie lassen sich eigentlich die Daten aus einer Cloud löschen?

Löschen ist nicht nur ein Klick

Auf den ersten Blick ist das Löschen von Daten auf dem eigenen Rechner dem Löschen in der Cloud sehr ähnlich. Man sucht im Programmmenü den Löschbefehl und klickt darauf. Doch weder auf dem eigenen Computer noch in der Cloud bedeutet der Befehl „Löschen", dass die Daten wirklich umgehend gelöscht sind. Bei einem Windows-Rechner landen die Daten in aller Regel im Papierkorb des Computers. Und von dort könnte man sie ohne größeren Aufwand wiederherstellen.

Bei einer Cloud ist dies nicht anders: Löschen bedeutet nicht, dass die Daten sofort und endgültig aus dem Cloud-Speicher verschwunden sind. Denn wie beim PC gibt es auch hier die Option, die Daten wiederherzustellen. Wie geht dann aber das „richtige" Löschen? Google hat das genaue Verfahren für die Google Cloud Plattform (GCP) ausführlich beschrieben.

Endgültiges Löschen in der Cloud kann Monate dauern

Ohne jeden Einzelschritt zu betrachten, lässt sich sagen, dass bei Google – und ebenso bei vielen anderen Cloud-Anbietern – das Löschen nur Schritt für Schritt geht. Entsprechend lange dauert es. So befinden sich die Cloud-Daten aus Gründen der Verfügbarkeit und Ausfallsicherheit bei Google nicht nur auf einem Cloud-Server, sondern auf mehreren. Bis der Löschauftrag für bestimmte Cloud-Daten wirklich alle Speicherorte erreicht hat und dort umgesetzt wurde, können zwei Monate vergehen, so Google. Da sich die Daten dann auch noch in Backups befinden können, dauert das Löschen insgesamt bis zu sechs Monate. Das zeigt, dass Daten auch in der Cloud nicht wirklich sofort gelöscht sind.

Wichtig: Sperren der Daten

Wichtig ist es deshalb, dass die Daten ab dem Moment des Löschauftrags gesperrt sind, also nicht mehr genutzt werden können. Laut Google wird dies unter anderem durch eine Verschlüsselung der zu löschenden Daten erreicht. Wie genau das Löschen funktioniert und wie lange es dauert, sollte man also seinen Cloud-Anbieter fragen.

Unternehmen sollten Cloud-Dienste also nur nutzen, wenn auch das Löschverfahren den Datenschutzvorgaben entspricht. Im Idealfall prüft und zertifiziert dies eine unabhängige Stelle. Die Google Cloud zum Beispiel hat, wie mehrere andere Cloud-Anbieter auch, vom BSI, dem Bundesamt für Sicherheit in der Informationstechnik, das sogenannte C5-Testat erhalten. Dabei wird auch das Löschverfahren überprüft. Trotzdem sollten Unternehmen immer das jeweilige Datenschutzkonzept hinterfragen.

Wissen Sie, wie Daten aus einer Cloud gelöscht werden?

Frage: ***Drückt man den Befehl „Löschen" in der Cloud-Applikation, sind die Daten aus der Cloud verschwunden. Stimmt das?***

a. **Nein, der Löschvorgang erfordert viele Schritte und dauert lange.**
b. **Ja, es könnte aber noch Kopien auf dem Endgerät geben.**

Lösung: Die Antwort a. ist richtig, die Antwort b. aber teilweise auch. Cloud-Daten sind nach dem Löschauftrag nicht sofort gelöscht. Es gibt viele Datenkopien auf verschiedenen Cloud-Servern und meistens auch im Backup des Cloud-Dienstes. Antwort b. ist insofern richtig, als es auch Datenkopien auf dem Endgerät und im Firmennetzwerk geben kann. Das Datenlöschen ist also immer ein komplexer Prozess, bei dem Cloud-Nutzer viele Speicherorte berücksichtigen müssen.

Frage: ***Können Daten nicht sofort gelöscht werden, dürfen sie weiterverarbeitet werden. Stimmt das?***

a. **Ja, was nicht gelöscht ist, lässt sich weiter nutzen. Die Verarbeitung endet dann mit dem Löschen.**
b. **Nein, wenn eine Löschpflicht besteht, das Löschen aber dauert, müssen die Daten gesperrt werden.**

Lösung: Hier ist die Antwort b. richtig. Sobald die Löschverpflichtung eintritt, dürfen Unternehmen die Daten nicht mehr verwenden. Die Daten müssen gegen eine weitere Nutzung geschützt, also gesperrt werden, zum Beispiel durch Verschlüsselung. Es gibt Ausnahmen von der Löschpflicht, etwa wenn die Verarbeitung erforderlich ist, um das Recht auf freie Meinungsäußerung auszuüben. Details finden sich in Artikel 17 der DSGVO.