Newsletter Datenschutz

Ausgabe Juni | 2018

CURACON
SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

Sanovis
Consulting with Care

Newsletter der Sanovis GmbH

Liebe Leserin, lieber Leser,

die neue Ausgabe des Datenschutz-Newsletters befasst sich mit zwei wichtigen Themen der Datenschutz-Grundverordnung: mit den Daten auf Papier, die auch geschützt werden müssen, und mit dem richtigen Löschen von Daten. Außerdem erfahren Sie, was es mit den Apps bei Facebook und anderen sozialen Netzwerken auf sich hat und wie die Fahrzeugvernetzung sowie smarte Apps auch in ältere Automobile Einzug halten – mit Folgen für den Datenschutz, die Sie nicht übersehen dürfen.

Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

Ihr Dr. Uwe Günther, Geschäftsfeld Datenschutz, Sanovis GmbH

Die DSGVO und Daten auf Papier

Der Datenschutz soll uns vor „Gefahren der EDV" bewahren – so hört man es häufig. Dabei gehen von Daten auf Papier oft viel größere Risiken für den Schutz personenbezogener Daten aus. Deshalb gilt die Datenschutz-Grundverordnung (DSGVO) auch für Daten auf Papier.

EDV = böse, Papier = harmlos?

Sie wollen nicht glauben, dass Daten auf Papier für den Datenschutz gar nicht so harmlos sind? Dann stellen Sie sich einfach zwei Fragen:

- Sehen Sie es Daten auf Papier an, ob jemand diese Daten gelesen hat?
- Sehen Sie es Daten auf Papier an, ob jemand das Papier kopiert hat?

Beide Fragen sind natürlich mit Nein zu beantworten. Wären die Daten statt auf Papier in elektronischer Form gespeichert, sähe das Ganze etwas anders aus. Lesezugriffe lassen sich genauso einfach protokollieren wie ein Download von Daten. Ob jemand erlaubt gehandelt hat oder nicht, kommt im Ernstfall daher schnell ans Licht

Papier ist nicht „besser"!

Klar, lückenlos funktioniert auch das nicht. So könnte jemand, der dazu berechtigt ist, Daten am Bildschirm aufrufen. Dann könnte er mit seinem Smartphone ein Foto des Bildschirms machen. Und schon hätte er das Verbot, die Daten zu kopieren, umgangen. Dennoch ändern solche Ausnahmefälle nichts am Prinzip: Personenbezogene Daten auf Papier sind mindestens genauso gefährdet wie elektronische Daten, wenn nicht sogar noch viel stärker!

Schreiben als Speicherung von Daten

Die DSGVO hat daraus die nötigen Folgerungen gezogen. Sie gilt unabhängig davon, ob Daten auf Papier gespeichert sind oder in elektronischer Form. Sie haben richtig gelesen: Auch das Festhalten von Daten auf Papier, ob mit Bleistift oder Drucker, bezeichnet die DSGVO als Speicherung von Daten! Das wirkt auf den ersten Blick ungewohnt. Aber wenn man kurz überlegt, ist das nur konsequent.

Schreiben als Verarbeitung von Daten

Haben Sie diese gedankliche Hürde genommen, fallen Ihnen einige andere Aspekte der DSGVO nicht mehr schwer. Die DSGVO gilt ausdrücklich auch für die „nicht automatisierte Verarbeitung personenbezogener Daten". So sagt es Art. 2 Abs. 1 DSGVO. Eine Form der Verarbeitung ist die Speicherung. Das definiert Art. 4 Nr. 2 DSGVO. Aus beidem zusammen folgt: Wer Daten auf Papier festhält, verarbeitet diese Daten, und zwar nicht automatisiert.

Notizzettel = „Dateisystem"?

Heißt das, man muss nun für jeden Notizzettel die DSGVO beachten? So weit geht die DSGVO nicht. Falls Daten nicht automatisiert verarbeitet werden, findet die DSGVO nämlich nur Anwendung, wenn

die Daten „in einem Dateisystem gespeichert sind." So sagt es Art. 2 Abs. 1 DSGVO.

Sie verzweifeln allmählich etwas, weil das schon wieder ein neuer Begriff ist? Keine Sorge! Dieser Begriff ist klar definiert: Ein „Dateisystem" ist jede strukturierte Sammlung personenbezogener Daten (Art. 4 Nr. 6 DSGVO). Beispiele für solche strukturierten Sammlungen sind Karteien und Hängeregistraturen, aber auch alphabetisch sortierte Unterlagen in Ordnern. Ein ungeordneter Haufen mit Notizzetteln fällt also nicht unter die DSGVO. Datenschutzgerecht entsorgen sollten ihn bitte trotzdem!

Die DSGVO und die Löschung von Daten

Daten löschen? Das machen wir jeden Tag! Irgendwelche Probleme dabei? Nein, wieso? So laufen typische Dialoge ab, wenn man dieses Thema in Unternehmen anspricht. Aber ganz so einfach war es schon bisher nicht, und die Datenschutz-Grundverordnung (DSGVO) bringt außerdem noch einige Neuerungen.

„Löschen" – gar nicht so einfach!

Was bedeutet es eigentlich, Daten zu löschen? Das Verschieben der Daten in einen elektronischen Papierkorb reicht jedenfalls nicht aus. Das dürfte jedem klar sein. Oder vielleicht doch nicht? Nur zur Sicherheit: Wenn Sie Daten mit ein paar Mausklicks „wiederherstellen" können, sind sie nicht wirklich gelöscht. Sie sind dann nur an einer anderen Stelle als bisher gespeichert, eben im „Papierkorb".

Löschen als Zerstörung

Aber was heißt Löschen dann? Der Europäische Gerichtshof verwendet klare Worte, um den Begriff „Löschen" verständlich zu erklären. Daten sind dann gelöscht, wenn sie „zerstört" sind. Die Daten dürfen also auf keinem Weg mehr rekonstruierbar/wiederherstellbar sein.

Daten auf Papier

Bei Daten auf Papier bedeutet dies beispielsweise, das Papier zu verbrennen. Zerkleinern kann man es natürlich auch. Aber das muss so geschehen, dass niemand mehr die Seiten wieder zusammensetzen kann. Unterschiede danach, wie schutzwürdig die Daten sind, macht das Recht dabei nicht. Für alle personenbezogenen Daten gelten bei einer Löschung vielmehr dieselben Regeln. Dies ist für viele noch ungewohnt und kann auch recht teuer werden. Aber so ist es eben.

Elektronische Daten

Elektronische Daten lassen sich auf den ersten Blick recht schnell löschen. Eine Möglichkeit ist das Überschreiben. Der Teufel steckt dabei im Detail. Viele Löschfunktionen bewirken lediglich, dass die entsprechenden Bereiche auf dem Datenträger (etwa einer Festplatte) nicht mehr gegen ein Überschreiben geschützt sind. Das heißt allerdings noch lange nicht, dass sie auch tatsächlich bald überschrieben werden. Manchmal geschieht dies auch nie. Wundern Sie sich also nicht, wenn die EDV erklärt, dass das Löschen von Daten nicht so banal ist, wie viele denken.

Gesetzliche Anlässe zur Löschung

Wann Daten gelöscht werden müssen, ist in Art. 17 DSGVO ausführlich geregelt. Zumindest die wichtigsten Fälle der Löschungspflicht sollte man kennen:

Rechtswidrige Verarbeitung

Wenn Daten unrechtmäßig verarbeitet wurden, müssen sie ohne Ausnahme gelöscht werden. Ein klassisches Beispiel: Um bestimmte Daten überhaupt verarbeiten zu dürfen, hat ein Unternehmen die Einwilligung der betroffenen Personen eingeholt. Leider stellt sich heraus, dass dabei rechtliche Fehler passiert sind und dass die Einwilligung unwirksam ist. Die Folge: Die betroffenen Daten sind zu löschen!

Widerruf einer Einwilligung

Ein nicht ganz so klassisches Beispiel: Jemand hat eine Einwilligung erteilt und widerruft sie. Welche Folgen hat das? Der Ausgangspunkt ist klar: Alles, was bis zum Widerruf mit den Daten geschehen ist, bleibt rechtmäßig. So regelt es Art. 7 Abs. 3 Satz 2 DSGVO.

Folgen eines Widerrufs

Aber wie sieht es ab dem Widerruf aus? Müssen die Daten jetzt gelöscht werden? Nicht so ohne Weiteres! Denn vor allem im geschäftlichen Bereich kann es nötig sein, die Daten noch länger vorrätig zu halten. Das gilt in erster Linie dann, wenn Buchführungspflichten oder steuerliche Pflichten das Unternehmen dazu zwingen.

Das sind dann rechtliche Verpflichtungen, gegen die das Unternehmen nichts machen kann. Die Folge: Weil es um die Erfüllung einer rechtlichen Verpflichtung geht (in diesem Fall gegenüber dem Staat), dürfen die Daten noch gespeichert werden, solange diese Pflicht besteht (Art. 17 Abs. 3 Buchst. b DSGVO). Der Widerruf der Einwilligung ändert daran nichts.

Zweckbindung

Doch Vorsicht: Die Speicherung ist nur genau für die Pflicht erlaubt, die erfüllt werden muss. Unzulässig wäre es beispielsweise, die Daten noch zu verwenden, um dem Kunden Werbematerial zuzuschicken. Die Verwendung für diesen Zweck muss ausgeschlossen werden. Die DSGVO spricht hier von einer „Einschränkung der Verarbeitung" (so die Überschrift von Art. 18 DSGVO). Früher bezeichnete man dies meist als „Sperrung".

Vorsicht vor Bußgeldern!

Solche und ähnliche Fälle zeigen, dass eine Löschung nicht nur technisch schwierig sein kann, sondern auch in rechtlicher Hinsicht ganz erhebliche Fragen aufwirft. Man sollte sie in jedem Fall ernst nehmen. Denn zumindest, wenn grobe Fehler passieren, kann dies durchaus zu einem Bußgeld seitens der Datenschutzaufsicht führen.

Datenrisiken bei Facebook & Co.: Wenn Apps zu Freunden werden

Der Datenskandal um Facebook und Cambridge Analytica sorgte für viele Schlagzeilen. Doch es darf nicht nur um diesen einen Fall gehen. Sondern es muss generell um die Datenfreigaben und um Apps in sozialen Netzwerken gehen.

Lehren aus dem Facebook-Skandal ziehen

Sicherlich erinnern Sie sich an Facebook und Cambridge Analytica. Die Datenschutzaufsichtsbehörden mahnen jedoch an, nicht nur diesen Einzelfall zu sehen. So gravierend die Vorwürfe dabei sein mögen, dürfen sie nicht darüber hinwegtäuschen, dass sie vermutlich nur ein kleines Puzzleteil des datenschutzrechtlich problematischen Geschäftsmodells von entsprechenden Unternehmen sind, erklärte kürzlich die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff.

Die Diskussion um Facebook und Cambridge Analytica sei nur ein Beispiel für die vielen datenschutzrechtlichen Risiken, denen Internetnutzerinnen und -nutzer alltäglich ausgesetzt sind. Als eine Folge der fortschreitenden Digitalisierung würden immer mehr Datenspuren hinterlassen, die mittels Big-Data-Technologie verknüpft werden können, um aussagekräftige Profile zu bilden.

Zentral: das Prinzip hinter Facebook-Apps

Auch wenn Cambridge Analytica inzwischen den Betrieb einstellen musste, ist es wichtig, sich das grundsätzliche Prinzip hinter Facebook-Apps anzusehen. Denn genau auf diesem Weg, mit einer Facebook-App, hatte Cambridge Analytica Zugang zu Nutzerdaten erhalten.

Apps wollen nicht nur spielen

Zuerst ist es entscheidend, zu verstehen, dass es hier nicht um die Facebook-App geht, die Sie vielleicht auf Ihrem Smartphone oder Tablet installiert haben. Vielmehr geht es um solche Apps, die Anwendungen innerhalb von sozialen Netzwerken wie Facebook sind. Die meisten Apps innerhalb von Facebook sind Spiele-Apps, doch darf man solche Apps nicht unterschätzen. Sie bieten nicht nur Spiele an, sondern sie erhalten Zugriff auf Daten der Nutzer und deren Kontakte. Man kann sich vorstellen, dass eine Facebook-App ähnliche Einsichten erhält wie eine Person, die man als Facebook-Freund oder -Freundin akzeptiert. Im Unterschied zu einer solchen Person beschafft sich eine App die verfügbaren Daten automatisiert.

„Digitale Enteignung"?

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz schrieb hierzu: „Cambridge Analytica hat sich mit simplen Mechanismen Zugang zu den bei Facebook vorhandenen Daten verschafft." Zudem warnte er: „Facebook ist nicht nur eine harmlose Plattform für die Vermittlung von Nachrichten, sondern eine Datenkrake, die mit den Daten ihrer Nutzerinnen und Nutzer Geschäfte macht. Die bei Facebook vorhandenen Daten können von anderen in einer Art und Weise gebraucht werden, die unkontrollierbar und evtl. sogar rechtswidrig ist. Der jetzige Skandal um Facebook ist eine absehbare Folge der ‚digitalen Enteignung', der die Nutzer des sozialen Netzwerks unterzogen werden."

Datenfreigaben bei Apps kontrollieren

Viele Werbetreibende interessieren sich für Facebook-Apps, da sie wertvolle Informationen bereitstellen können. Facebook selbst schreibt: „Millionen Unternehmen jeder Größe verwenden die Facebook Apps und Services, um auf jedem Gerät eine Verbindung zu echten Menschen herzustellen."

Welche Daten geben Facebook-Apps weiter?

Verhindert der Nutzer die Datenfreigabe nicht, können Facebook-Apps zum Beispiel folgende Informationen weitergeben: demografische Merkmale wie Alter, Geschlecht, Ausbildung, Interessen des Nutzers, basierend auf den Interessen und Aktivitäten auf Facebook, sein Kaufverhalten, verwendete Geräte sowie Personen, denen die App gefällt, und sogar deren Freunde.

Das Spielen mit Facebook-Apps kann also deutliche Folgen für den Datenschutz haben. Sehen Sie sich deshalb Ihre Datenschutz-Optionen in Facebook an und besuchen Sie das sogenannte Appcenter in Facebook, um zu sehen, mit welchen Apps Sie bereits befreundet sind.

Nicht nur Facebook-Apps hinterfragen

Denken Sie aber nicht nur an die Apps innerhalb von Facebook; auch andere soziale Netzwerke haben Apps. Ebenso gibt es Apps innerhalb des von Ihnen verwendeten Webbrowsers und in vielen Cloud-Services, die Sie vielleicht schon nutzen.

Apps sind weit verbreitet und stellen nichts anderes dar als Anwendungen, die Daten verarbeiten. Apps – und zwar jede Form von Apps – müssen deshalb daraufhin hinterfragt werden, welche Daten sie zu welchem Zweck verarbeiten und weitergeben und wie sie die Daten schützen wollen. Leider sucht man heute noch bei vielen Apps vergeblich nach einer Datenschutzerklärung. Können Sie den Datenschutz bei einer App nicht klären, verzichten Sie lieber auf die App – auf dem Smartphone, auf dem Tablet, in Facebook und ganz generell bei jeder App.

Impressum

Redaktion:
Dr. Uwe Günther
Sanovis GmbH

Anschrift:
Richard-Strauss-Straße 69
81679 München

Telefon: 0 89 / 9927579 22
E-Mail: Uwe.Guenther@sanovis.com

Datenschutz in Fahrzeugen: Nicht nur an neue Firmenwagen denken

Vernetzte Fahrzeuge sind weder Zukunftsmusik, noch sind die Datenrisiken auf kostspielige Neuwagen beschränkt. Jedes Fahrzeug, privat oder geschäftlich, kann zu einem Connected Car werden. Machen Sie sich mit den Folgen vertraut!

Digitalisierung der Fahrzeugbranche

Wer eine Automobilmesse besucht, trifft dort häufig auf Facebook und Google, und wer die Hallen einer IT-Messe betritt, sieht eine große Zahl an Fahrzeugen an den Messeständen. Vernetzte Fahrzeuge, auch Connected Cars genannt, gehören zu den Top-Trends. Doch nicht nur die Industriebranchen haben großes Interesse, auch die Nutzer sind aufgeschlossen, wie Umfragen zeigen.

Ob optimale Routenplanung und Navigation oder der Einsatz von autonomen Fahrzeugen auf der Straße: Die Mehrheit der Bundesbürger wünscht sich laut Digitalverband Bitkom den Einsatz von Künstlicher Intelligenz (KI), um den Verkehrsfluss zu optimieren und Unfälle zu vermeiden. So halten es 58 Prozent für sinnvoll, mithilfe von KI selbstfahrende Fahrzeuge auf die Straße zu bringen.

Rund 9 von 10 Unternehmen der Automobilbranche (86 Prozent) fordern eine gesetzliche Verpflichtung, anonymisierte Fahrzeugdaten bereitzustellen. Dabei sagt jedes vierte Unternehmen (25 Prozent), es sollten alle Daten zur Verfügung gestellt werden müssen, 61 Prozent plädieren für ausgewählte Daten.

Fahrzeugdaten sind Thema für den Datenschutz

In vernetzten Autos entsteht eine Vielzahl von Daten, etwa zur Motorleistung, zum Fahrverhalten oder auch zur Position des Fahrzeugs. Der großen Mehrheit der Bürger ist es wichtig zu wissen, welche Daten erzeugt werden (83 Prozent) und wer sie nutzt (93 Prozent), so der Bitkom-Verband. Dabei fordern die meisten, dass der Eigentümer des Fahrzeugs (69 Prozent) bzw. der Fahrer (57 Prozent) entscheiden soll, wer die Daten nutzen darf. 28 Prozent wollen diese Entscheidung dem Gesetzgeber überlassen, nur zwei Prozent dem Automobilhersteller.

Die Aufsichtsbehörden für den Datenschutz haben bereits mehrfach auf die Datenrisiken durch die Fahrzeugvernetzung hingewiesen: In modernen Fahrzeugen sammeln bereits heute unzählige Sensoren Daten zum Fahrverhalten und den zurückgelegten Wegen, so die Aufsichtsbehörden. Daraus lassen sich detaillierte Persönlichkeitsprofile erstellen. Fahrerinnen und Fahrer müssen daher jederzeit die volle Hoheit über die Verwendung personalisierbarer Fahrzeugdaten haben. Grundsätzlich sollten sie über jede Datenverwendung im Sinne einer vollständigen Transparenz unterrichtet werden. Damit dies möglich ist, sind datenschutzgerechte Technologien und Voreinstellungen notwendig.

Achtung: Nicht nur moderne Fahrzeuge betroffen

Das Thema „Vernetzte Fahrzeuge" ist inzwischen nicht mehr auf moderne Firmenwagen beschränkt, auch wenn auf den Messen immer die neusten Modelle an den Ständen stehen.

Vorhandene Entertainment-Systeme im Auto, Freisprechanlagen und Navigationssysteme lassen sich leicht um neue Funktionen ergänzen, durch Upgrades, durch die Verknüpfung via Bluetooth oder USB-Stecker mit dem Smartphone des Fahrers oder der Fahrerin, aber auch durch neue Lösungen, die einfach in den Zigarettenanzünder im Altfahrzeug gesteckt werden und dann einen digitalen Assistenten wie Siri, Alexa oder Google Assistant an Bord holen.

Wenn Sie also in einen älteren Firmenwagen einsteigen, kann auch dies ein vernetztes Fahrzeug sein. Die Digitalisierung macht vor älteren Fahrzeugen nicht zwingend halt. Fragen Sie deshalb, was das Fahrzeug alles kann, das Sie nutzen wollen, und seien Sie kritisch bei neuen Geräten, die Sie in dem Fahrzeug, das Sie nutzen, anbringen wollen.

Haben Sie Ihre Daten im Griff? Testen Sie sich!

Frage: ***Vernetzte Fahrzeuge sind moderne Automobile, die bereits ab Werk Internet-anschluss und Bordcomputer haben. Stimmt das?***

a. **Nein, jedes Fahrzeug lässt sich vernetzten, auch nachträglich.**
b. **Ja, denn alte Fahrzeuge haben keine Verbindung zum Internet.**

Lösung: Die Antwort a. ist richtig. Selbst ein Oldtimer kann zum Connected Car gemacht werden. Dafür reicht schon ein kleines Gerät, das an den Zigarettenanzünder angesteckt wird und die Sprachsteuerung des Autoradios ermöglichen soll.

Frage: ***Fahrzeugdaten sind unkritisch, denn die Personen, die fahren, werden dort ja nicht genannt. Stimmt das?***

a. **Ja, vernetzte Fahrzeuge liefern nur Daten zur Motorleistung und zum aktuellen Verbrauch des Automobils.**
b. **Nein, je nach Anwendung können auch zum Beispiel Standortdaten gesammelt werden, die Bewegungsprofile ermöglichen. Über ein gekoppeltes Smartphone oder durch Registrierung für eine Auto-App entsteht dann ein Bezug zu den Personendaten.**

Lösung: Hier ist die Antwort b. richtig. Die Aufsichtsbehörden für den Datenschutz warnen davor, dass aus den Daten der Fahrzeugvernetzung Rückschlüsse auf die Personen gezogen werden können. Aus Fahrzeugprofilen lassen sich oftmals Nutzerprofile generieren. Dazu kann bereits die Installation einer App unter einem bestimmten Nutzerkonto reichen. Auch bei Fahrzeug-Apps kommt es auf die Prüfung der Datenschutzerklärung an!