Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2018

Liebe Leserin, lieber Leser,

strenggenommen geht es mit den neuen Datenschutzgesetzen nun in die heiße Phase: Die DSGVO ist in Kraft und manche Themen klären sich erst jetzt so richtig in der Praxis.

Ein Beispiel ist der Umgang mit Apps, die für uns längst zum Alltag gehören. Dabei sind uns als Anwender die Datenrisiken oftmals nur in Teilen oder gar nicht bewusst. Mehr zu diesem Thema können Sie gleich hier auf der ersten Seite lesen.

Bislang hörte man meist nur von Themen zum Schutz vor „Gefahren der EDV", doch die Datenschutz-Grundverordnung gilt nicht nur für die technische Verarbeitung von personenbezogenen Daten, sondern auch für Daten auf Papier. Mehr Informationen hierzu und zu möglichen Risiken, finden Sie auf Seite 5.

Weitere Themen in dieser Ausgabe sind die Anonymisierung von Daten mit ihren Vor- und Nachteilen und die Verschlüsslung von E-Mails.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

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.

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,

In dieser Ausgabe:

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, sein Kaufverhalten basierend auf den Interessen und Aktivitäten auf Facebook, 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 sie. 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 ihnen – 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 Anwendungen vergeblich nach einer Datenschutzerklärung. Können Sie den Datenschutz bei einer App nicht klären, verzichten Sie lieber auf diese – auf dem Smartphone, auf dem Tablet, in Facebook und ganz generell bei jeder App. &

3

Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2018

ALTHAMMER & KILL

Neu und wichtig: Europäischer Datenschutzausschuss

EU-Gremien sind für viele etwas, das sie kaum überblicken. Da kann es eher zu Unlust führen, wenn noch eine neue Einrichtung dazukommt. Dennoch: Ist demnächst öfter vom Europäischen Datenschutzausschuss die Rede, sollten Sie lieber einmal hinhören. Was er sagt, wird beruflich wie privat oft wichtig sein.

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO). Das hat besonders in Deutschland so große öffentliche Aufmerksamkeit gefunden, dass die Abkürzung DSGVO für viele inzwischen etwas völlig Gewohntes ist.

Eine neue europäische Institution

Eines ist dabei in der Berichterstattung aber nahezu untergegangen: In Brüssel hat eine neue Einrichtung ihre Tätigkeit aufgenommen. Sie trägt die Bezeichnung „Europäischer Datenschutzausschuss".

Mitglieder des Ausschusses

Fragt man, wer in diesem Ausschuss sitzt, fällt die Antwort so aus: Jeder Mitgliedstaat der EU darf ein Mitglied in den Ausschuss entsenden. Dabei muss es sich um den Leiter einer Aufsichtsbehörde handeln. Für Deutschland wird dies die Bundesbeauftragte für den Datenschutz sein. So legt es das neue Bundesdatenschutzgesetz 2018 fest. Hinzu kommt als Mitglied noch der Europäische Datenschutzbeauftragte. Er kümmert sich um den Datenschutz in den Einrichtungen der EU selbst, also etwa um den Datenschutz in den Dienststellen der Europäischen Kommission in Brüssel. Bei dem Ausschuss geht es also ersichtlich darum, den Sachverstand der Aufsichtsbehörden auf europäischer Ebene zu bündeln.

29 Mitglieder – also nur endlose Diskussionen?

Insgesamt ist der Ausschuss somit relativ groß. Denn schließlich hat die EU (mit Großbritannien) 28 Mitgliedstaaten, und der Europäische Datenschutzbeauftragte kommt als Ausschussmitglied Nr. 29 hinzu. Das

kann auf den ersten Blick den Eindruck erwecken, dass in diesem Ausschuss nur viel geredet wird, ohne dass dies praktische Folgen hätte.

Aufgabe des Ausschusses

Nun: Geredet wird dort bestimmt viel werden. Das ist übrigens auch gut so, denn es stehen wahrhaft genügend Probleme im europäischen Datenschutz an. Aber diese Diskussionen werden auch handfeste Folgen haben. Das liegt an der Aufgabe, die der Ausschuss hat.

Einheitliche Anwendung der DSGVO

Generell besteht die Aufgabe darin, die einheitliche Anwendung der DSGVO in der EU sicherzustellen. Ein wichtiges Instrument hierfür werden Leitlinien und Empfehlungen sein, die der Ausschuss aufstellt. Dazu gehören ausdrücklich auch Leitlinien für die Festsetzung von Geldbußen bei Datenschutzverstößen.

Mit anderen Worten: Der Ausschuss wird erheblichen Einfluss darauf haben, unter welchen Voraussetzungen es konkret zu Geldbußen kommt und wie hoch die Geldbußen ausfallen.

Förderung von Siegeln und Prüfzeichen

Außerdem soll der Ausschuss Datenschutzsiegel und Datenschutzprüfzeichen fördern. Sie können für Unternehmen, aber natürlich auch für Privatpersonen ein wichtiger Hinweis darauf sein, ob ein Anbieter von Dienstleistungen die DSGVO einhält. Der Druck, solche Siegel und Prüfzeichen einzuführen, ist erheblich. Viele Unternehmen versprechen sich davon einen Wettbewerbsvorteil.

Vorlage von Zweifelsfragen an den Ausschuss

Nationale Aufsichtsbehörden, aber auch die Europäische Kommission können dem Ausschuss Zweifelsfragen zur Beurteilung vorlegen. Damit die Antwort nicht zu lange auf sich warten lässt, darf die Europäische Kommission eine Frist setzen, innerhalb derer der Ausschuss Stellung nehmen soll. Dabei muss die Kommission begründen, warum sie die Frage für so dringlich hält.

Einflussmöglichkeiten für Unternehmen

Wichtig für Unternehmen, aber auch für Verbände: Der Ausschuss kann „interessierte Kreise“ konsultieren. Mit anderen Worten: Hier besteht die Möglichkeit, Argumente einzubringen und die Beratungen zu beeinflussen. Der Ausschuss ist verpflichtet, die Ergebnisse einer solchen Konsultation zu veröffentlichen.

Transparenz der Tätigkeit

Auch die Stellungnahmen und Empfehlungen des Ausschusses müssen veröffentlicht werden. Das ermöglicht eine öffentliche Diskussion. Wenn es um Themen geht, die zahlreiche Verbraucher oder Unternehmen betreffen, werden sie mit Sicherheit ihren Weg in die Medien finden.

Jahresbericht

Als wäre dies alles nicht schon genug, ist der Ausschuss auch noch verpflichtet, einen Jahresbericht zu erstellen. Mancher wird argwöhnen, dass ein solches Dokument voraussichtlich am Tag nach seiner Veröffentlichung wieder vergessen ist. Dagegen spricht, dass der gebündelte Sachverstand aller Datenschutz-Aufsichtsbehörden in der EU ein recht hohes Gewicht haben dürfte. Einfach eben mal ignorieren wird man ihn deshalb kaum können. &

5 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2018

ALTHAMMER & KILL

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.

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?

EDV = böse, Papier = harmlos?

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 und mit seinem Smartphone ein Foto des Bildschirms machen. So 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! &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, Thomas Althammer

Gestaltung: Ralf Winternheimer
www.winternheimer.net

Fotos Mini-Figuren: © Katja Borchhardt
www.miniansichten.de

Anschrift:
Althammer & Kill GmbH & Co. KG
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Schutzgebühr Print-Ausgabe: 10,– €

Kirchlicher Datenschutz – auch für Ungläubige!

Kirchlicher Datenschutz scheint auf den ersten Blick ein Thema nur für besonders fromme Menschen zu sein. Ein „gewöhnliches Kirchenmitglied" hat damit doch nichts zu tun. Und jemand, der aus der Kirche ausgetreten ist, schon gar nicht? Urteilen Sie nicht voreilig! Denn auch Ungläubige können beispielsweise in ein kirchlich geführtes Krankenhaus kommen. Und schon haben sie mit dem kirchlichen Datenschutz zu tun.

Mit Religion und Kirchen haben Sie nichts am Hut? Das ist Ihr gutes Recht. Denn in Deutschland herrscht Freiheit des Glaubens und der Religion. Dazu gehört auch die Freiheit, sich damit nicht zu befassen oder beispielsweise die großen Kirchen ausdrücklich abzulehnen.

Nutzung kirchlicher Einrichtungen – Kindergarten, Krankenhaus & Co.

Dennoch lassen sich Kontakte mit kirchlichen Einrichtungen manchmal schlicht nicht vermeiden. Bei kirchlichen Kindergärten mag dies noch möglich sein. Denn schließlich können Sie Ihr Kind auch anderswo betreuen lassen.

Bei der Einlieferung in ein kirchliches Krankenhaus nach einem Unfall wird es schon schwieriger. Kaum jemand wird sich dagegen wehren, wenn er dort schnelle Hilfe erhält. Und das Unternehmen, in dem Sie tätig sind, wird Aufträge von Kirchen im Normalfall auch nicht ablehnen.

Umgang mit personenbezogenen Daten

Oft genug geht es dann nicht ohne personenbezogene Daten. Am Beispiel des kirchlichen Krankenhauses wird das besonders deutlich. Natürlich dokumentieren kirchliche Krankenhäuser die Behandlung eines Patienten nach denselben Maßstäben wie andere Krankenhäuser auch. Sie verfügen also über Gesundheitsdaten und weitere persönliche Daten (etwa Name und Anschrift) des Patienten – mag er nun Kirchenmitglied sein oder nicht.

Rolle der Datenschutz-Grundverordnung

Damit stellt sich die Frage, welche Regeln in Kirchen für den Schutz personenbezogener Daten gelten. Müssen Kirchen schlicht und einfach die Datenschutz-Grundverordnung (DSGVO) beachten? Oder dürfen sie eigene Regeln schaffen? Dürfen solche Regeln möglicherweise sogar der DSGVO widersprechen?

Eigene Datenschutzregelungen von Kirchen

Die letzte Frage ist mit einem klaren Nein zu beantworten. Die DSGVO lässt nicht zu, dass sich Kirchen eigenes Recht schaffen, das der DSGVO widerspricht. Aber bekanntlich sind viele Regeln der DSGVO sehr allgemein, sodass an diesen Stellen Handlungsspielräume bestehen. Die DSGVO sagt dies in Art. 91 sinngemäß so: Kirchen und religiöse Vereinigungen dürfen eigene Datenschutzregelungen haben. Sie müssen aber umfassend sein und außerdem mit der DSGVO in Einklang stehen.

Kaum inhaltliche Überraschungen

Entsprechend wenige Überraschungen bietet der Text kirchlicher Datenschutzgesetze. Er stimmt weitgehend mit der Datenschutz-Grundverordnung überein. Das könnte den Eindruck vermitteln, als sei das ganze Thema nur etwas für Spezialisten. Denn wenn am Ende dasselbe herauskommt, kann es letztlich ja gleichgültig sein, welcher Paragraf aus welchem Gesetz angewandt wird, oder?

Eigene Datenschutzaufsicht von Kirchen

Diese Schlussfolgerung wäre voreilig. Das zeigt sich spätestens, wenn sich ein Betroffener über Datenschutzverstöße beschweren will. Angenommen, Betroffener ist ein Patient, der in einem kirchlichen Krankenhaus behandelt worden ist. Er muss sich mit seiner Beschwerde an die Datenschutzaufsicht der Kirche wenden, zu der das Krankenhaus gehört. Staatliche Datenschutzaufsichtsbehörden sind in diesem Fall nicht zuständig.

Dies gilt unabhängig davon, ob der Patient selbst der Kirche angehört oder nicht. Es genügt, dass er die Dienste einer kirchlichen Einrichtung in Anspruch genommen hat. Damit gelten für ihn die kirchlichen Datenschutzregelungen.

Ungewohnt, aber konsequent

Das mag ungewohnt wirken. Ob es im Ergebnis stört, ist eine andere Frage. Das wäre wohl nur der Fall, wenn das Ergebnis anders ausfällt als sonst, weil eine kirchliche Einrichtung mit im Spiel ist. Genau dies kann allerdings durchaus vorkommen! Deutlich zeigt sich dies wieder am Beispiel des kirchlichen Krankenhauses.

Angenommen, jemand wird in einem „gewöhnlichen" Krankenhaus behandelt. Und weiter angenommen, es gibt für dieses Krankenhaus einen Krankenhausseelsorger. Dann darf dieser Seelsorger nur dann über den Aufenthalt eines Patienten im Krankenhaus informiert werden, wenn der Patient damit ausdrücklich einverstanden ist.

Liegt derselbe Patient dagegen in einem kirchlichen Krankenhaus, sieht die Sache völlig anders aus. Vom Selbstverständnis einer solchen Einrichtung her ist es völlig in Ordnung, dass ein Seelsorger auch unaufgefordert einmal vorbeischaut und dabei den Namen des Patienten kennt. Aufdrängen wird er seine Dienste aber natürlich nicht. &

Was sind anonyme Daten, und was bringen sie überhaupt (noch)?

Die Anonymisierung von Daten erscheint vielen Unternehmen wie eine Entwertung. Doch Anonymisierung hat auch Vorteile: Anonyme Daten unterliegen nicht dem Datenschutz. Sollten Unternehmen also zur Anonymisierung greifen? Und wann sind Daten wirklich anonymisiert?

Die Datenschutz-Grundverordnung (DSGVO) greift immer dann, wenn sich Daten auf eine identifizierte oder identifizierbare natürliche Person beziehen. Entsprechend besagt die DSGVO: Die Grundsätze des Datenschutzes gelten nicht für anonyme Informationen, also für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder für personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass sich die betroffene Person nicht oder nicht mehr identifizieren lässt.

Offensichtlich sind anonyme Daten ein Königsweg, um die hohen Anforderungen aus der DSGVO zu erfüllen. Denn Unternehmen müssen die Grundsätze des Datenschutzes dann – zumindest für diese Daten – gar nicht beachten. Doch Vorsicht: Ganz so einfach ist es nicht. Zuerst steht die Prüfung an, ob tatsächlich anonyme Daten vorliegen, bevor man die DSGVO zur Seite legt.

Wann lassen sich Daten tatsächlich als anonym werten?

Nur wenn wirklich erfolgreich anonymisiert wird, müssen die Vorgaben

des Datenschutzes nach DSGVO für diesen Fall nicht weiter beachtet werden. Die DSGVO sagt, wann man von einer Anonymisierung ausgehen kann: So wurde nur dann anonymisiert, wenn es keine Mittel zur Identifizierung einer natürlichen Person mehr gibt, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine natürliche Person direkt oder indirekt zu identifizieren.

Keine solcher Mittel gibt es, wenn die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand zu hoch wären. Dabei ist immer zu berücksichtigen, was die aktuell verfügbare Technologie zu leisten vermag. Man kann davon ausgehen, dass die Mittel zur Identifizierung mit der Zeit immer günstiger und schneller werden, da sich die Technologie weiterentwickelt.

Wissen Sie, wann man von anonymen Informationen spricht? Machen Sie den Test!

Frage: Werden keine Namen und Vornamen der Personen gespeichert, sind die Daten anonym. Stimmt das?

a. Nein, es gibt viel mehr Informationen, mit denen sich Personen identifizieren lassen.
b. Ja, ohne Namen sind Daten anonym.

Lösung: Die Antwort a. ist richtig. Die DSGVO besagt: Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Frage: Wenn eine Lösung Anonymisierung verspricht, liefert sie auch anonyme Daten. Stimmt das?

a. Ja, jedes Werkzeug zur Anonymisierung erzeugt anonyme Informationen.
b. Nein, je nach Lösung können die Personen trotzdem identifizierbar sein.

Lösung: Hier ist die Antwort b. richtig. Die DSGVO macht deutlich, dass man mit gewissen Anstrengungen und technologischen Mitteln unter Umständen die Personen trotz eines Anonymisierungsversuchs identifizieren kann. Nur dann, wenn es keine Mittel zur Identifizierung einer natürlichen Person mehr gibt, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, liegt eine Anonymisierung vor, wenn also der Aufwand und die Kosten zu hoch für eine Identifizierung wären. Dies hängt allerdings von der technologischen Entwicklung ab, ändert sich also mit der Zeit.

Entsprechend muss man jeweils zum gegenwärtigen Zeitpunkt prüfen, ob natürliche Personen noch identifizierbar sind oder nicht, wenn man sich für eine Methode zur Anonymisierung entscheidet.

Anonymisierung ist sinnvoll

Auch wenn nicht jede beliebige Methode zur Anonymisierung ausreicht, lohnt es sich für Unternehmen, sich mit den Möglichkeiten zur Anonymisierung zu befassen. Vielfach besteht immer noch die Meinung, anonyme Daten seien wertlos für betriebliche Auswertungen. Tatsächlich aber können viele Analysen und Statistiken ohne jeden konkreten Personenbezug für das Unternehmen hilfreich und nützlich sein.

Unternehmen erheben zum Beispiel regelmäßig Daten zur Kundenpflege und -bindung. Häufig werden diese Daten auch zur Analyse des Kundenverhaltens wie zur Identifizierung von Zusammenhängen und Hintergründen von Käufen genutzt, um damit Marketing- und Vertriebstätigkeiten strategisch zu planen und zu unterstützen. Dafür werden die Namen der Betroffenen jedoch nicht benötigt.

So ist es für die Erfolgskontrolle einer Marketing-Aktion unerheblich, ob es Herr Maier oder Frau Schulze waren, die gekauft haben. Es ist vielmehr entscheidend, zu welcher Altersgruppe die Käufer zählen, ob sie eher online oder im stationären Geschäft gekauft haben und wie schnell sie auf die Werbung reagiert haben. Für all diese Informationen braucht man kein Wissen über die konkreten Personen. Anonymisierung bedeutet also nicht Entwertung, sondern hilft dem Datenschutz und damit dem Unternehmen. &

E-Mail-Verschlüsselung: Was fordert der Datenschutz?

Die Datenschutz-Grundverordnung (DSGVO) nennt Verschlüsselung als Maßnahme für die Sicherheit der Verarbeitung personenbezogener Daten. Müssen deshalb alle E-Mails von nun an verschlüsselt werden?

Wenn Sie eine Computer-Zeitschrift zur Hand nehmen, begegnen Ihnen in der letzten Zeit viele Werbeanzeigen, die aussagen, mit der DSGVO sei nun die Zeit gekommen, dass alle E-Mails komplett verschlüsselt werden müssen, vom Absender bis zum Empfänger (Ende-zu-Ende-Verschlüsselung).

So wichtig eine Verschlüsselung im Internet auch ist: So mancher Anbieter von Verschlüsselungslösungen übertreibt und verkürzt die Forderungen der Datenschutz-Grundverordnung derart, dass man den Eindruck bekommen kann, unverschlüsselte E-Mails zu verschicken, wäre grundsätzlich eine Datenschutzverletzung. Das stimmt so nicht!

Es kommt weiter auf den Schutzbedarf an

Bereits das alte Bundesdatenschutzgesetz nannte die Verschlüsselung als eine der zentralen technisch-organisatorischen Maßnahmen. Verschlüsselung hatte und hat eine wichtige Stellung. Sie trägt dazu bei, das Schutzziel „Vertraulichkeit“ zu erreichen.

Außerdem hilft sie, die Integrität und Echtheit von Daten zu prüfen. Trotzdem gilt: Geeignete technische und organisatorische Maßnahmen sollen ein Schutzniveau gewährleisten, das dem Risiko angemessen ist. Sie sollen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ausgewählt werden.

Bedeutet das nun, dass E-Mail-Verschlüsselung freiwillig ist? Nein, natürlich nicht. Es kommt auf den genauen Fall an.

Was Aufsichtsbehörden dazu sagen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit in NRW schreibt zum Beispiel: Maßnahmen wie „Verschlüsselung“ sind als Beispiele für Standardmaßnahmen zu verstehen. Das heißt: Sofern ihr Einsatz möglich und angemessen ist, sind sie grundsätzlich umzusetzen.

Es kommt also auf die Angemessenheit und damit den Schutzbedarf an. Sollen Daten mit hohem oder sehr hohem Schutzbedarf, wie etwa Gesundheitsdaten, per E-Mail verschickt werden, ist eine Ende-zu-Ende-Verschlüsselung erforderlich. Da die Betreffzeile einer E-Mail nicht durch Ende-zu-Ende-Verschlüsselung geschützt wird, ist sicherzustellen, dass sie keine Daten mit hohem oder sehr hohem Schutzbedarf enthält.

Bei der Übermittlung personenbezogener Daten mit normalem Schutzbedarf besteht die Möglichkeit, dass im Einzelfall der Verzicht auf eine Ende-zu-Ende-Verschlüsselung der Inhaltsdaten statthaft ist. Als Mindeststandard ist bei der Übermittlung personenbezogener Daten mit normalem Schutzbedarf eine Transportverschlüsselung erforderlich, so die Aufsichtsbehörde.

Es zeigt sich: Es kommt auf den Schutzbedarf der personenbezogenen Daten und die Art der Verschlüsselung an. Alle E-Mails zu verschlüsseln, fordert der Datenschutz also nicht. &

Alles nur geklaut? Sichere Dateiablage in der Cloud.

Es klingt zunächst paradox: Unternehmensinterne Daten sollen auf öffentlichen Servern gespeichert werden, um sie dort von überall abrufen zu können. Für einen gelungenen Drahtseilakt zwischen erhöhter Flexibilität und sicherer Verschlüsselung soll dieser Beitrag Ihnen hilfreiche Tipps geben.

Die Grundlage eines sicheren Datenaustausches ist die dabei genutzte Verschlüsselung. Moderne Verfahren beruhen auf kryptographischen Schlüsseln, die für die Ver- und Entschlüsselung verwendet werden.

Wenn nur die Anwender Zugriff auf diese Schlüssel haben, der Serverbetreiber bei der Schlüsselverwaltung außen vor bleibt und die Ver- und Entschlüsselung auf den Geräten der Anwender durchgeführt wird, dann spricht man von einer Ende-Zu-Ende Verschlüsselung. In diesem Fall ist sichergestellt, dass nur die Anwender Zugriff auf die gespeicherten Daten haben. Dies gilt auch für den Fall, dass der Serverbetreiber gehackt wird und die verschlüsselten Daten ausgeleitet werden. Da der entsprechende Schlüssel nur auf dem Client verfügbar ist, können gestohlene Daten nicht entschlüsselt werden.

Zwei Faktoren für mehr Sicherheit

Abgesehen von der genutzten Verschlüsselung lässt sich die Sicherheit durch weitere Zusatzfunktionen, wie eine Zwei-Faktor-Authentifizierung steigern. Hierbei wird neben einem Passwort eine weitere Information oder ein physisches Gerät benötigt, um auf die gespeicherten Daten zuzugreifen. Kommen also die Zugangsdaten eines Benutzers abhanden, so ist ein unberechtigter Zugriff nicht möglich, da der zusätzliche Faktor benötigt wird.

Neben den Sicherheitsanforderungen sollte auch die Flexibilität der betrachteten Lösung berücksichtigt werden. Gerade bei einer Ende-Zu-Ende Verschlüsselung ist es häufig notwendig, dass ein anbieterspezifischer Client installiert wird. Dies ist zu berücksichtigen, wenn beispielsweise häufig mit Geschäftspartnern Daten ausgetauscht werden sollen, da in diesem Falle auch die Partner diesen Client installieren müssen.

Kein direkter Zugriff für US-Behörden

Als großer Softwarehersteller bietet Microsoft seine verschlüsselte Online-Plattform OneDrive an. Diese wurde in Deutschland über ein Treuhändlermodell in Zusammenarbeit mit der Deutschen Telekom vertrieben, wodurch DSGVO-konform ein direkter Zugriff für US-Behörden unterbunden wurde. Dieses Treuhändlermodell wurde nun abgekündigt und es bleibt abzuwarten, wie Microsoft OneDrive in Zukunft datenschutzkonform eingesetzt werden kann.

Auch Lösungen von Anbietern wie Dropbox sollten nur nach genauer Prüfung eingesetzt werden. Zwar ist ein datenschutzkonformer Einsatz aktuell theoretisch möglich, da Dropbox Teilnehmer am US-Privacy Shield ist, allerdings ist der Fortbestand dieser Lösung aufgrund von anhaltender Kritik ungewiss.

Lösungen zur Speicherung von Daten existieren nicht nur von kommerziellen Anbietern, sondern auch Open-Source-Lösungen wie ownCloud bzw. NextCloud sind verfügbar. Diese bieten den Vorteil, dass die gesamte Verarbeitung der gespeicherten Daten unter der eigenen Kontrolle erfolgen und dass die Software auf die eigenen Anforderungen angepasst werden kann. Mit dieser Flexibilität geht allerdings auch ein erhöhter Aufwand für den Betrieb einher. Hinsichtlich der Zuverlässigkeit haben diese Lösungen mittlerweile einen Reifegrad erreicht, welcher durchaus mit kommerziellen Anbietern mithalten kann.

Welche Lösung für Ihre Anwendungszwecke am besten geeignet ist, lässt sich nicht pauschal beantworten, da jede Lösungen Vor- und Nachteile besitzen kann. &

Benötigen Sie weitere Informationen?

Wir freuen uns über Ihre Kontaktaufnahme:
info@althammer-kill.de

11 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2018

ALTHAMMER & KILL

News

Aus unserem aktuellen Newsletter:

Althammer & Kill ist Rahmenvertragspartner des Deutschen Paritätischen Wohlfahrtsverbandes
https://www.althammer-kill.de/news-detail/rahmenvertragspartner-des-deutschen-paritaetischen-wohlfahrtsverbandes/

Herausforderungen Datenschutz
https://www.althammer-kill.de/news-detail/herausforderungen-datenschutz/

Mitarbeiter im Datenschutz unterweisen
https://www.althammer-kill.de/news-detail/mitarbeiter-im-datenschutz-unterweisen/

Joint Control in der Datenschutz-Grundverordnung – Alles neu, aber auch alles ungeklärt?
https://www.althammer-kill.de/news-detail/joint-control-in-der-datenschutz-grundverordnung/

Verpflichtung auf das Datengeheimnis – Was ändert sich mit der Datenschutz-Grundverordnung?
https://www.althammer-kill.de/news-detail/verpflichtung-auf-das-datengeheimnis/

Anmeldemöglichkeiten zum Newsletter finden Sie unter:
www.althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

17.–19.09.2018, Hildesheim
BeB-Fachtagung Dienstleistungsmanagement 2018
Wir sind auch dieses Jahr wieder Partner der BeB-Fachtagung „Dienstleistungsmanagement" und beteiligen uns mit dem Vortrag „Digitalisierung und das Datenschutzgesetz der EKD – Wie passt das zusammen?"

18.10.2018, Hannover / 24.10.2018, Leipzig / 22.11., Regensburg
Vincentz Akademie:
„Die Datenschutz-Grundverordnung in der Altenpflege"
Seit dem 25.05.2018 ist die Datenschutzgrundverordnung (DSGVO) in Kraft und bringt neben vielen Neuerungen auch empfindlich erhöhte Bußgelder mit sich. Ist Ihre Einrichtung bereits fit und in der Lage, die Vorgaben zu erfüllen und somit Bußgelder und Imageschäden abzuwehren?

07.–08.11.2018, Nürnberg
ConSozial 2018
Die ConSozial 2018 – Wir freuen uns auf Ihren Besuch!

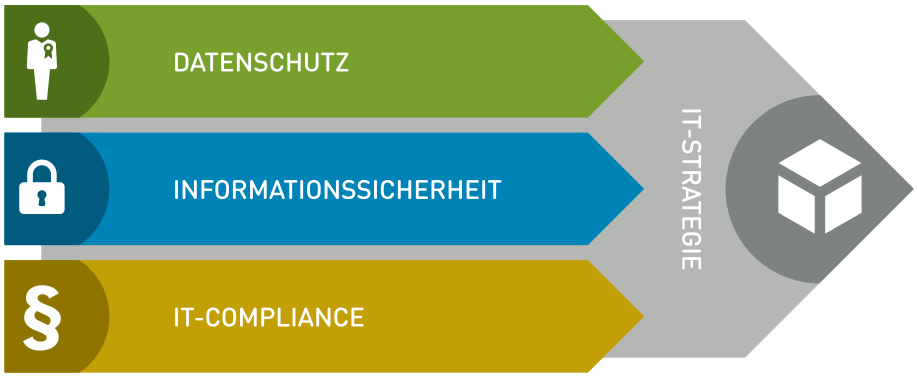
13.–15.11.2018, Paderborn
Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Datenschutz auf Basis von DSGVO/BDSG (neu), DSG-EKD und KDG

20.–22.11.2018, Paderborn
Ausbildung IT-Sicherheitsbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Informationssicherheit auf Basis von IT-Grundschutz und der IT-Sicherheitsverordnung (ITSVO-EKD)

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern die passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten Sie bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ).

Althammer & Kill GmbH & Co. KG

Standort Hannover:
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Standort Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0

Standort Mannheim:
Kaiserring 10–16 · 68161 Mannheim
Tel. +49 621 121847-0

info@althammer-kill.de
www.althammer-kill.de

Mitglied im:

FINSOZ e.V. · GDD Mitglied · BvD e.V. Mitglied · Hannover IT