Newsletter Datenschutz

Ausgabe August | 2018

CURACON
SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

Sanovis
Consulting with Care

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

bereits seit dem 25. Mai 2018 gilt nun die Datenschutz-Grundverordnung (DSGVO). Trotzdem kursieren noch viele Mythen über das neue Datenschutzrecht im Internet, in Zeitungen und in Diskussionen. Die neue Ausgabe des Datenschutz-Newsletters klärt deshalb darüber auf, wann und wie E-Mails wirklich zu verschlüsseln sind, um dem Datenschutz gerecht zu werden. Ebenso stellt die neue Ausgabe klar, dass der kirchliche Datenschutz für jeden relevant sein kann, ob man nun in die Kirche geht oder nicht.

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, Geschäftsfeld Datenschutz, Sanovis GmbH

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?

Werbung übertreibt gern

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 auf 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.

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.

Eine neue europäische Institution

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. 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.

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.

Freiheit von Glauben und Religion

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. An dieser Stelle bestehen Handlungsspielräume. 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, der Betroffene 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.

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

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?

DSGVO gilt nicht für anonyme Informationen

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 solchen 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.

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.

**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.