Newsletter Datenschutz

Ausgabe Februar | 2019

Newsletter der Curacon GmbH Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

Fehler passieren immer wieder, auch im Datenschutz. Die neue Ausgabe Ihrer Datenschutz-Zeitung zeigt Ihnen Beispiele für solche Fehler und hilft dabei, Fehler schneller zu erkennen. So erfahren Sie, warum es falsch wäre, Datenrisiken nur in digitalen Bereichen zu suchen. Ein weiterer Fehler ist es, dass viele Unternehmen glauben, sie würden für jede Datenverarbeitung eine Einwilligung benötigen.

Kommt es tatsächlich einmal zu einem Fehler, dann sollten Sie wissen, welche Aufgaben Sie haben, damit die Datenpanne korrekt gemeldet wird. Zudem ist es wichtig, zu verstehen, wie sich Fehler im Datenschutz, die bei einem Geschäftspartner auftreten, auf den eigenen Datenschutz auswirken können. Sonst besteht die Gefahr, dass aus einer Lieferkette eine Fehlerkette wird.

Wir wünschen Ihnen viel Spaß beim Lesen!

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

Ihr Stefan Strüwe, Geschäftsfeldleiter Datenschutz, Curacon GmbH

2019: Neues Jahr, neue Datenrisiken?

Auch für 2019 haben IT-Sicherheitsexperten wieder ihre Prognosen veröffentlicht über neue Risiken, die personenbezogene Daten bedrohen. Es wäre aber falsch, sich nun besonders auf diese Risiken zu konzentrieren.

Die Zeichen stehen auf Sturm

Gleich, ob Sie sich die Vorhersagen der Sicherheitsbehörden oder der Sicherheitsanbieter für 2019 ansehen: Kaum ein Security-Experte ist der Meinung, dass die Risiken für personenbezogene und andere zu schützende Daten geringer werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von einer Gefährdungslage auf einem neuen Niveau. Cyber-Angriffe werden 2019 noch intelligenter und ausgereifter, erklären auch die Forscher von Fortinet. Zieht man Parallelen zu den Wetterprognosen, lässt sich sagen, die Sicherheitsspezialisten erwarten eine Zunahme von schweren Unwettern.

Nicht an die steigenden Risiken gewöhnen

Die Berichte der Security-Experten rund um den Jahreswechsel bekommen in den Medien immer viel Aufmerksamkeit. Doch besteht die Gefahr, dass wir Menschen uns daran gewöhnen, dass die Gefahren aus dem Internet und für unsere Daten immer größer werden. Tatsächlich nehmen die Risiken für personenbezogene Daten stetig zu. Die Prognosen der McAfee Labs für 2019 besagen zum Beispiel: Neue mobile Malware wird Smartphones, Tablets und Router austesten, um Zugang zu den digitalen Assistenten, die sie kontrollieren, und zu heimischen IoT-Geräten (IoT = Internet of Things) zu erhalten. Smart Homes werden verstärkt zum Angriffsziel. Was bedeutet das nun konkret für den Datenschutz im neuen Jahr?

Die Risiken folgen der Digitalisierung

Nutzen Unternehmen und Privatpersonen vermehrt Dienste aus der Cloud, werden Smartphones und Tablets für immer mehr Menschen zum stetigen Begleiter und die Wohnungen immer vernetzter, dann zieht das Angriffswellen auf sich. Überall, wo neue Bereiche digitalisiert werden, ist mit Angriffen der Internetkriminellen zu rechnen.

Doch auch abseits der digitalen Technik lauern Gefahren

Man darf aber nicht vergessen, dass Staat, Wirtschaft und Gesellschaft bei Weitem noch nicht angekommen sind an dem Ziel der digitalen Transformation. Viele Verfahren und Prozesse sind seit Jahren unverändert im Einsatz. Dadurch sind sie aber nicht aus dem Fokus der Angreifer. Die Sicherheitsexperten stellen fest, dass Internetkriminelle mit den klassischen Kriminellen zusammenarbeiten. Jede der kriminellen Seiten lernt und profitiert von der anderen. Deshalb muss weiterhin damit gerechnet werden, dass klassische Einbrüche stattfinden, um an vertrauliche Informationen zu kommen, und nicht nur Hacker-Attacken.

Nur weil die Sicherheitsprognosen die neuen Technologien und ihre Risiken betonen, nehmen die Gefahren in den klassischen Bereichen nicht ab. Im Jahr 2019 muss mit allen bisherigen Bedrohungen gerechnet werden, die wir schon seit vielen Jahren kennen – die neuen Bedrohungen kommen hinzu. Sehen Sie deshalb jede Sicherheitsprognose wie eine Fortsetzungsgeschichte: Es werden neue Kapitel geschrieben, ohne dass man die alten einfach zuschlagen dürfte.

Einwilligung – nötig oder nicht?

„Wenn man Daten von Kunden oder Mitarbeitern verarbeiten will, braucht man jetzt immer erst einmal eine Einwilligung!" So ist es derzeit oft zu hören. Aber stimmt das wirklich?

Wunderliche Erlebnisse

Erlebnisse dieser Art waren in den letzten Monaten alltäglich:

- Ein Mann geht zum selben Arzt wie immer. Jetzt soll er plötzlich eine „Einverständniserklärung in die Datenverarbeitung" unterschreiben. Sonst könne man ihn leider nicht mehr behandeln, erklärt ihm die Arzthelferin.
- Eine Frau will wie gewohnt im Herbst in der Autowerkstatt die Reifen wechseln und bis zum nächsten Frühjahr lagern lassen. Auf einmal soll das nur noch möglich sein, wenn sie eine „Einwilligung in die Datenverarbeitung" unterschreibt.

Beides ergibt keinen Sinn. Warum?

Vertrag als Rechtsgrundlage

Autowerkstatt und Kunde haben einen Vertrag. Vereinbart sind Reifenwechsel und Einlagerung der Reifen. Damit das möglich ist, braucht die Werkstatt einige Daten des Kunden, vor allem seinen Namen sowie die Anschrift und/oder die Telefonnummer. Denn die Rechnung muss an eine bestimmte Person adressiert sein. Und wie soll der Kunde im nächsten Frühjahr die eingelagerten Reifen wiederbekommen, wenn man ihn nicht namentlich kennt?

Ähnlich sieht es beim Arzt aus. Zu einer Behandlung gehört es, dass sie dokumentiert wird. Die Dokumentation muss natürlich dem Patienten persönlich zuzuordnen sein. Dazu braucht der Arzt dessen Namen und darüber hinaus auch das Geburtsdatum, um Verwechslungen auszuschließen. Was dokumentiert werden muss, ist eine medizinische Frage, je nach Krankheit. Die Befugnis zur Dokumentation an sich ergibt sich aber stets aus dem Behandlungsvertrag.

Regelung in der DSGVO

Das alles folgt eigentlich schon aus dem gesunden Menschenverstand. Denn wer einen Vertrag schließt, dem ist klar: Wenn sein Vertragspartner persönliche Daten braucht, um die vereinbarte Leistung erbringen zu können, dann muss es erlaubt sein, diese Daten zu verarbeiten. Aber selbstverständlich gibt es auch einen Paragrafen dazu. Es handelt sich dabei um Art. 6 Abs. 1 Satz 1 Buchstabe b der Datenschutz-Grundverordnung (DSGVO). Demnach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn diese Verarbeitung erforderlich ist „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist."

Diese Regelung passt auf beide Beispiele. Sie gilt nämlich für Verträge aller Art, egal ob es dabei um eine ärztliche Behandlung oder um einen Reifenwechsel geht.

Bitte eines Interessenten um Prospekte

Aber wie sieht es aus, wenn keinerlei Vertrag besteht? Ist zumindest dann immer eine Einwilligung notwendig? Nein, auch dann nicht. Beispiel: Eine Interessentin bittet ein Unternehmen, das Natur-textilien verkauft, darum, ihr Kataloge und Prospekte zuzusenden. Damit die Zusendung möglich ist, muss das Unternehmen Name und Anschrift der Interessentin verwenden, um ein Kuvert zu beschriften. Das ist eine Form der Verarbeitung personenbezogener Daten. Genau das wollte die Interessentin jedoch ganz offensichtlich!

Deshalb ist dafür nicht noch zusätzlich eine Einwilligung erforderlich. In der Sprache der DSGVO ist die Beschriftung des Kuverts zur „Durchführung einer vorvertraglichen Maßnahme erforderlich, die auf Anfrage der betroffenen Person erfolgt". Keine einfache Formulierung, aber im Ergebnis völlig klar!

Gesetzliche Arbeitnehmerpflichten

Beispiele dafür, dass eine Einwilligung überflüssig ist, gibt es auch im Arbeitsleben. So mag es sein, dass es einem Arbeitgeber eigentlich ziemlich gleichgültig ist, ob ein Mitarbeiter einer Kirche angehört oder nicht. Sollte der Mitarbeiter allerdings Mitglied einer Religionsgemeinschaft sein, die Kirchensteuer erhebt, dann muss der Arbeitgeber die Kirchensteuer abführen. Damit er dies tun kann, muss die Kirchenmitgliedschaft in den Personalunterlagen festgehalten sein. Auf eine Einwilligung des Arbeitnehmers kommt es dabei nicht an. Der Arbeitgeber braucht die Daten nämlich, um eine rechtliche Verpflichtung zu erfüllen (siehe Art. 6 Abs. 1 Buchstabe c DSGVO).

Keine Einwilligung „nur zur Sicherheit"!

Mancher mag sich fragen, ob man nicht trotzdem zumindest immer noch zusätzlich eine Einwilligung einholen sollte, einfach „zur Sicherheit".

Die Antwort darauf ist ein klares Nein. Denn eine Einwilligung kann jederzeit ohne jeden Grund widerrufen werden (Art. 7 Abs. 3 Satz 1 DSGVO). Und wie bitte sollte man einem Kunden oder einem Mitarbeiter dann folgenden Ablauf erklären: Erst bittet man ihn um eine Einwilligung. Diese Einwilligung widerruft er. Aber den Widerruf ignoriert man dann einfach mit der Begründung, dass die Verarbeitung auch ohne Einwilligung gesetzlich erlaubt ist. Das wird auch ein gutwilliger Mensch nicht verstehen.

Meldung von Datenpannen

Die DSGVO hat die Meldepflicht für Datenpannen wesentlich verschärft. Was geht das den „normalen Mitarbeiter" an? Deutlich mehr, als viele glauben!

Versendungspannen sind Klassiker

Versendungspannen gehören zu den häufigsten Datenpannen. Einer der Klassiker: Eine E-Mail soll an eine größere Zahl von Adressaten gehen. Sie sollen nichts voneinander wissen. Doch statt im bcc-Feld landet die Adressatenliste versehentlich im cc-Feld. Die Folge: Jeder Adressat sieht die E-Mailadressen aller anderen Adressaten!

Eher selten nötig: Benachrichtigung der betroffenen Personen

Rückgängig machen lässt sich das nicht mehr. Also rasch eine Entschuldigungsmail an alle Adressaten und alles ist gut? So einfach ist es nicht! Rechtlich gesehen stellt eine solche E-Mail eine Benachrichtigung der betroffenen Personen dar. Eine solche Benachrichtigung wäre jedoch oft gar nicht nötig. Vorgeschrieben ist sie laut Datenschutz-Grundverordnung (DSGVO) nur, wenn die Datenpanne für die betroffenen Personen voraussichtlich ein „hohes Risiko" zur Folge hat (Art. 34 Abs. 1 DSGVO). Doch das ist eher selten der Fall.

Angenommen, es geht um eine Liste von Personen, die regelmäßig Sonderangebote per E-Mail erhalten. Dann liegt im Normalfall kein hohes Risiko vor. Denn was soll hier schon passieren? In solchen Fällen ist eine Benachrichtigung eine Frage der Höflichkeit, nicht eine Frage des Rechts.

Stets eilig: Meldung an die Datenschutzaufsicht

Viel wichtiger ist eine Meldung der Datenpanne an die Datenschutzaufsicht. Für sie gilt:

- Grundsätzlich ist eine solche Meldung bei jeder Datenpanne erforderlich.
- Eine Ausnahme greift nur dann, wenn die Panne voraussichtlich zu keinerlei Risiko für die betroffenen Personen führt.

Die tückische 72-Stunden-Frist

Hinzu kommt noch folgende Tücke: Für die Benachrichtigung der betroffenen Personen ist keine Frist vorgeschrieben, für die Meldung der Datenpanne an die Datenschutzaufsicht dagegen schon! Sie muss im Normalfall binnen 72 Stunden erfolgen (Art. 33 Abs. 1 DSGVO).

Keine Meldung durch einzelne Mitarbeiter!

Die Meldung an die Aufsichtsbehörde erfolgt dabei nicht durch den Mitarbeiter, der die Panne verursacht hat! Sie ist vielmehr vom Unternehmen zu veranlassen. Wer innerhalb des Unternehmens zuständig ist, legt die Unternehmensleitung fest.

Verschweigen? Lieber nicht!

Das scheint auf den ersten Blick Möglichkeiten der Manipulation zu bieten. Sollte man vielleicht möglichst lange Stillschweigen über eine Datenpanne bewahren? Sorgt das dann dafür, dass die 72-Stunden-Frist nicht zu laufen beginnt? Solche Überlegungen sind gefährlicher Unfug. Angenommen, die Unternehmensleitung erfährt erst nach Wochen von einer Datenpanne, meldet sie dann aber sofort an die Aufsichtsbehörde. Hier ist zwar die Meldepflicht formal gesehen erfüllt. Die Aufsichtsbehörde wird dem Unternehmen aber vorwerfen, dass die interne „Pannenorganisation" mangelhaft ist. Denn sonst hätte die Unternehmensleitung sofort von der Panne erfahren.

Regeln für Mitarbeiter

Die Regeln für jeden einzelnen Mitarbeiter lauten daher:

1) Kehren Sie Datenpannen nie unter den Tisch!

2) Informieren Sie vielmehr sofort die Vorgesetzten!

3) Ist kein Vorgesetzter greifbar, kann der Datenschutzbeauftragte weiterhelfen.

4) Verschweigen macht alles nur schlimmer!

Wichtige Unterschiede

Wichtig ist, dass die Meldung an die Datenschutzaufsicht und die Benachrichtigung der betroffenen Personen zunächst einmal nichts miteinander zu tun haben. Die Meldung an die Datenschutzaufsicht muss immer rasch erfolgen. Dabei gilt der Grundsatz: Lieber eine Meldung zu viel als eine Meldung zu wenig! Mit der Benachrichtigung der betroffenen Personen sieht es anders aus. Sie verlangt sorgfältige Überlegung und ist bewusst nicht an bestimmte gesetzliche Fristen gebunden.

Meldungen an die Aufsichtsbehörde sind in der Praxis sehr häufig, Benachrichtigungen betroffener Personen dagegen recht selten. Dieser Unterschied beruht zunächst einmal auf den unterschiedlichen gesetzlichen Regelungen. Er lässt sich aber auch aus der Sache leicht erklären:

- Bei der Datenschutzaufsicht arbeiten Profis. Sie können die Dinge einordnen. Wenn eine erste Meldung später teilweise korrigiert werden muss, löst das bei ihnen keine Unsicherheit aus.
- Anders dagegen die Situation der betroffenen Personen. Jede Benachrichtigung verunsichert sie. Sie fragen nach. Kommen dann nur unvollständige Informationen oder Informationen, die später korrigiert werden müssen, hilft ihnen das nicht weiter. Also muss hier gleich alles stimmen.

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

Datenschutz bei Geschäftspartnern: Worauf kommt es an?

Fehler bei einem Zulieferer können schwerwiegende Auswirkungen auf die eigenen Produkte haben. Das gilt nicht nur für das Qualitätsmanagement, sondern auch im Datenschutz. Nicht nur der Einkauf sollte daran denken, sondern jeder einzelne im Unternehmen.

Teile und Schwachstellen zukaufen

Stellen Sie sich vor, ein Bauteil, das von einem Zulieferer stammt, ist fehlerhaft, und es wird trotzdem in das neue Fahrzeug eingefügt. Die Folge ist, dass das Fahrzeug nun einen Fehler aufweist, der je nach Art des Bauteils dramatische Auswirkungen haben kann. Denken Sie nur einmal an ein Bauteil wie einen Bremsklotz. Der zugekaufte Fehler kann Menschenleben bedrohen.

Die Gefahr, über eingekaufte Leistungen und Produkte den eigenen Produkten und Services Schwachstellen und Fehler zuzuführen, besteht in jeder Branche. Deshalb fordern Richtlinien für ein Qualitätsmanagement immer, dass auch die Qualität bei den Zulieferern geprüft und überwacht werden muss. Das Gleiche muss im Datenschutz gelten.

Schlechter Datenschutz in der Lieferkette

Stellt ein Dienstleister oder Lieferant Ihres Unternehmens keinen angemessenen Datenschutz sicher, wirkt sich dies auch auf den Datenschutz in Ihrem Unternehmen aus. Hat der Lieferant Zugang zu den Kundendaten Ihres Unternehmens und sorgt selbst nicht für Datensicherheit, kann es passieren, dass ein Datendieb über die Schwachstellen Ihres Lieferanten an die Daten in Ihrem Unternehmen kommt.

Oder ein Softwaremodul, das Ihr Unternehmen nutzt, hat eine kritische Schwachstelle. Wenn Sie das Modul nutzen oder in andere Programme Ihres Unternehmens einfügen, dann lässt sich diese Schwachstelle bei Ihnen selbst ausnutzen. Eigentlich ist dies kein Geheimnis, und trotzdem achten zu wenige Unternehmen darauf, den Datenschutz bei ihren Geschäftspartnern zu hinterfragen, um den eigenen Datenschutz gewährleisten zu können.

Aufsichtsbehörde sieht Klärungsbedarf

Datenschutzbehörden wie das Landesamt für Datenschutzaufsicht in Bayern (BayLDA) haben festgestellt, dass Meldungen von Datenschutzverletzungen fast immer das jeweilige Unternehmen selbst als verantwortlich bezeichnen, kaum jedoch einen Geschäftspartner oder Dienstleister. Da nach der Datenschutz-Grundverordnung (DSGVO) auch Verletzungen der Sicherheit bei Dienstleistern (sogar bei weiterer Unterauftragsvergabe) eine Meldeverpflichtung auslöst, stellte sich dem BayLDA die Frage, wieso es kaum Meldungen gibt, die von (internationalen) Dienstleistern ausgelöst werden. Offensichtlich fehlt das Bewusstsein dafür, dass Datenschutzmängel bei Geschäftspartnern den eigenen Datenschutz betreffen. Die Ursachen für eine Datenschutzverletzung werden fast nur intern gesehen. Das entspricht aber nicht den Tatsachen. Deshalb sollte nicht nur der Einkauf, sondern jeder, der mit Dienstleistern und anderen Geschäftspartnern zu tun hat, daran denken, dass der Datenschutz auch dort stimmen muss, damit der eigene Datenschutz gewährleistet ist.

Kein Generalverdacht, sondern mehr Aufmerksamkeit

Es geht dabei nicht darum, jeden Geschäftspartner als Ursache von Datenschutzmängeln zu betrachten und bei Datenschutz-Problemen die Schuld immer bei anderen zu suchen. Vielmehr geht es darum, beim Datenschutz genau wie bei der Qualität immer die ganze Lieferkette im Auge zu behalten. Beziehungen zu Dienstleistern und Geschäftspartnern verdienen viel Aufmerksamkeit – auch im Sinne des Datenschutzes.

Kennen Sie die Risiken einer Lieferkette?

Machen Sie den Test!

Frage: ***Datenschutz-Probleme sind anders als Qualitätsmängel. Fehler im Datenschutz pflanzen sich nicht fort. Stimmt das?***

a. Nein, Schwachstellen im Datenschutz eines Partnerunternehmens können den eigenen Datenschutz bedrohen.

b. Ja, wer selbst einen guten Datenschutz hat, muss die Fehler der Lieferanten nicht fürchten.

Lösung: Die Antwort a. ist richtig. Doch obwohl es selbstverständlich sein sollte, dass sich Probleme im Datenschutz über die Lieferkette hinweg ausbreiten können, achten viele Unternehmen zu wenig auf das Datenschutzniveau der Geschäftspartner.

Frage: ***Jeder ist für seinen Datenschutz verantwortlich. Stimmt das?***

a. Ja, das stimmt, deshalb gibt es eine verantwortliche Stelle für den Datenschutz in jedem Unternehmen.

b. Nein, zusätzlich ist man auch verantwortlich dafür, nur mit solchen Dienstleistern zusammenzuarbeiten, die ein angemessenes Datenschutzniveau haben (Auftragsverarbeitung).

Lösung: Die Antworten a. und b. sind gemeinsam richtig, die Antwort a. ist falsch, wenn man sie alleinstehen lässt. Die Datenschutz-Grundverordnung (DSGVO) kennt neben der Verantwortung auch die gemeinsame Verantwortung und die Beschränkung auf solche Dienstleister für eine Auftragsverarbeitung, die einen angemessenen Datenschutz nachweisen können. Unter einer gemeinsamen Verantwortlichkeit versteht man: Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung personenbezogener Daten fest, so sind sie gemeinsam Verantwortliche. Dies kann in einer Kooperation entlang der Lieferkette schnell der Fall sein.