

Datenschutz *aktuell* - Ausgabe 02-2021

Der Datenschutz-Newsletter aus Nürnberg



Liebe Leserinnen und Leser,

in dieser 2. Ausgabe für das Jahr 2021 beschäftigen wir uns mit dem Thema "Datenpannen".

Gerade datenschutzrechtliche Datenpannen können vielschichtig sein und dürfen nicht unterschätzt werden. Verstöße, unter anderem gegen Betroffenenrechte, können zu empfindlichen Reaktionen der Datenschutzbehörden führen. Einer dieser Verstöße ist zum Beispiel die Nichtbeachtung oder verspätete Bearbeitung von Auskunftersuchen. Gerade um dieses Thema geht es im ersten Beitrag.

Viel Spaß beim Lesen und mit vielen Grüßen aus Nürnberg

Ihr Peter Brandmann
(Externer Datenschutzbeauftragter)

Datenauskunft als Datenpanne?



Die Umsetzung der DSGVO bereitet gerade bei den Betroffenenrechten weiterhin Probleme. So haben Unternehmen oftmals noch keinen richtigen Prozess, um Auskunftersuchen datenschutzgerecht nachzukommen. So muss etwa geklärt werden, ob die anfragende Person wirklich die betroffene Person ist.

Fristen einzuhalten ist nicht alles

Stellen Sie sich vor, Sie sollen einen Antrag auf Auskunft bearbeiten. Sie müssen feststellen, ob Ihr Betrieb personenbezogene Daten verarbeitet, die die anfragende Person betreffen. Ist das der Fall, klären Sie, welche Daten dies sind und zu welchem Zweck Ihr Betrieb sie verarbeitet. Sie bereiten nun eine Kopie der personenbezogenen Daten vor, die Gegenstand der Verarbeitung sind, um diese Informationen zur Verfügung zu stellen.

Dabei können Sie sich nicht beliebig Zeit lassen. Denn die Auskunft muss unverzüglich, also ohne schuldhaftes Zögern, erteilt werden, spätestens jedoch binnen eines Monats nach Eingang des Auskunftersuchens. Nun darf es aber nicht passieren, dass Sie möglichst schnell die Datenkopie verschicken – sonst könnte die Datenauskunft zu einer Datenpanne werden.

Die Identität des Antragstellers muss geklärt sein

Die Aufsichtsbehörden für den Datenschutz haben mehrfach deutlich gemacht: Es muss sichergestellt sein, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten.

Das bedeutet somit, dass Sie sicherstellen müssen, dass die Person, die die Auskunft wünscht, auch tatsächlich das Recht dazu hat, also tatsächlich die betroffene Person oder eine von der betroffenen Person bevollmächtigte Person ist. Das sollte jedes Unternehmen durch einen Prozess sicherstellen. Bei vielen Unternehmen ist dem aber noch nicht so, auch wenn die DSGVO bereits drei Jahre zur Anwendung kommt.

Nicht auf die falsche Prüfung der Identität setzen

Nun gibt es verschiedene Wege, um die Identität einer anfragenden Person zu überprüfen. Dabei muss dieser Weg zum einen datenschutzgerecht sein, also zum Beispiel keine unnötigen Daten abfragen. Zum anderen muss der gewählte Weg aber auch sicher genug sein.

Wenn Sie das Verfahren in Ihrem Unternehmen noch nicht kennen, erkundigen Sie sich bitte, bevor Sie ein Auskunftersuchen bearbeiten. Wichtig ist auch, dass Sie die Einschränkungen der Verfahren kennen, die gern in der Praxis genutzt werden.

Ob beispielsweise die Identifizierung über ein Nutzerkonto (also Benutzername und Passwort) sicher ist, hängt sehr stark vom Passwort ab, das der Nutzer vergeben hat. Ist es zu leicht zu knacken, können Angreifer Nutzerkonten übernehmen und damit weitere Daten ausspähen – womöglich dann über ein Auskunftersuchen mit gefälschter Identität.

Kennt also eine anfragende Person das Passwort der betroffenen Person, das für einen Online-Dienst Ihres Unternehmens besteht, und kann sie sich einloggen, bedeutet dies nicht, dass es wirklich die betroffene Person ist, die die Anfrage stellt. Seien Sie also vorsichtig, denn Identitätsdiebstahl im Internet greift um sich. So basieren die stark verbreiteten Phishing-Attacken genau auf einer gefälschten digitalen Identität, die Vertrauen erwecken und vertrauliche Daten herauslocken soll. Das Auskunftersuchen per Mail kann also auch eine Fälschung sein.

Ist es wirklich die betroffene Person? Machen Sie den Test!

Frage: Beantragt eine Person Auskunft über eine bekannte E-Mail-Adresse, kann man davon ausgehen, dass die Anfrage echt und berechtigt ist. Stimmt das?

1. Nein, denn die Absenderangaben können gefälscht sein.
2. Ja, aber nur, wenn es sich um eine verschlüsselte, signierte E-Mail des Absenders handelt.

Lösung: Die Antworten 1 und 2 sind richtig. Absenderangaben bei E-Mails lassen sich fälschen, dafür muss man nicht einmal das E-Mail-Passwort des Betroffenen haben, es reicht das Editieren der Absenderangaben im Mail-Programm des (kriminellen) Absenders. Konnten Angreifer aber das E-Mail-Passwort stehlen, kann die E-Mail sogar echt sein. Doch die Identität ist eine gestohlene und stimmt nicht. Der Bundesdatenschutzbeauftragte schreibt zum Auskunftsrecht: Es empfiehlt sich, die Auskunft schriftlich oder in einer sicheren elektronischen Form (etwa per De-Mail oder mittels verschlüsselter E-Mail über das Programm Pretty Good Privacy (PGP) oder GnuPG) anzufordern.

Frage: Die Kopie eines Personalausweises darf keine geschwärzten Stellen enthalten, wenn eine anfragende Person damit ihre Identität im Auskunftsverfahren nachweisen soll. Stimmt das?

1. Ja, die Kopie muss vollständig und gut zu lesen sein.

2. Nein, die Kopie muss leserlich sein, sie darf aber bestimmte Stellen enthalten, die geschwärzt wurden, weil sie für die Identitätsprüfung nicht notwendig sind.

Lösung: Die Antwort 2 ist richtig. Die Aufsichtsbehörden für den Datenschutz haben zum Thema „Kopie des Personalausweises“ darauf hingewiesen, dass man als Betroffener die nicht erforderlichen persönlichen Daten auf der Kopie des Ausweises (wie Augenfarbe, Größe, ID-Nummer, Unterschrift) schwärzen sollte. Andere Daten wie der Name und der Vorname dürfen natürlich nicht unkenntlich gemacht sein.

Datenpannen durch Fehlversendungen



Eine Mail mit personenbezogenen Daten geht per cc versehentlich an Adressaten, die sie gar nicht erhalten sollten. Personalunterlagen werden per Post an den falschen Herrn Meier geschickt. Alles nicht so schlimm? Eine kurze freundliche Entschuldigung, und alles ist wieder gut? So einfach ist es leider nicht!

Pflicht, Datenpannen zu melden

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Verpflichtung, Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde für den Datenschutz zu melden. Dies muss im Normalfall binnen 72 Stunden geschehen.

Eine Ausnahme hiervon gilt nur dann, wenn voraussichtlich nicht mit Risiken für die betroffenen Personen zu rechnen ist. So regelt es Art. 33 Abs. 1 DSGVO.

Jedes Unternehmen muss sich so organisieren, dass es Datenpannen tatsächlich bemerkt. Anders gesagt: Es muss seine Mitarbeiterinnen und Mitarbeiter dazu verpflichten, Datenpannen auch zu melden.

Vorbeugende Maßnahmen

Noch besser ist es natürlich, wenn solche Pannen erst gar nicht vorkommen. Die häufigste Art von Pannen sind Fehlversendungen. Das zeigen die Statistiken der Aufsichtsbehörden. Sie betreffen sowohl klassische Briefsendungen als auch Mails. Die Gründe sind jeweils unterschiedlich.

Pannen bei Briefsendungen

Bei Briefsendungen ist es schlicht so, dass vor allem jüngeren Mitarbeiterinnen und Mitarbeitern die Übung im Umgang mit Briefen fehlt. Privat schreiben sie kaum welche. Und im Unternehmen sind Briefe tendenziell ebenfalls seltener geworden.

Der Klassiker in diesem Bereich: Es müssen Unterlagen an eine größere Zahl von Adressaten verschickt werden. Auf den Unterlagen steht jeweils die Anschrift des Adressaten, und zwar fehlerfrei. Die Umschläge werden getrennt davon mit der jeweiligen Anschrift versehen. Beim Zusammenführen von Umschlägen und Unterlagen passieren dann die Fehler. Die Unterlagen kommen jeweils in den falschen Umschlag. Das geschieht besonders oft, wenn Praktikanten oder andere wenig geübte Personen damit beauftragt werden.

Schnell stellt sich dann heraus, dass auch solche scheinbar einfachen Arbeiten eben doch nicht „jeder kann“.

Fensterumschläge als Lösung?

Manche Aufsichtsbehörden empfehlen inzwischen, in solchen Fällen Fensterumschläge zu verwenden. Dann ist es nicht mehr nötig, die Umschläge gesondert zu beschriften. Vielmehr wird die entsprechende Unterlage so in den Umschlag hineingesteckt, dass die Anschrift im Brieffenster erscheint. Das ist an sich keine schlechte Idee. Freilich kann dabei ein anderes Problem auftauchen. Immer wieder beginnt nämlich der Text auf einer Unterlage so nah an der Anschrift, dass Teile des Textes im Brieffenster zu sehen sind. Auch wenn es sich banal anhört, ist hier also genaues Falten des Papiers gefragt. Das verlangt ebenfalls Übung.

Vier-Augen-Prinzip

Eine andere Möglichkeit wäre, nach dem Vier-Augen-Prinzip vorzugehen. Das bedeutet allerdings, dass jeder Brief von zwei Mitarbeitern in die Hand genommen werden muss. Dieser Aufwand ist oft schlicht zu groß.

Pannen bei E-Mails

Klassische Datenpannen beim Versand von E-Mails ist die versehentliche Nutzung der cc-Funktion anstelle der bcc-Funktion, um ein und dieselbe Mail an eine größere Zahl Adressaten zu schicken. Sie wissen nicht, was der Unterschied ist? Dann sollten Sie offen gesagt die Finger davon lassen, mit diesen Funktionen zu arbeiten.

Nur kurz zur Erinnerung: Bei der bcc-Funktion sieht ein Adressat die Mailadressen der anderen Adressaten nicht, bei der cc-Funktion dagegen schon. Auf diese Weise ist dann schnell einmal eine komplette Kundenliste offengelegt. Dadurch kann dann ein Problem entstehen, das weit über den Datenschutz hinausreicht.

Die Funktion „an alle“

Eine ausgesprochen tückische Funktion ist auch die Funktion „an alle“. Mit „alle“ sind dabei dann beispielsweise sämtliche Mitarbeiter eines Unternehmens gemeint, die ein Mailsystem benutzen. Das können Tausende von Mailadressen sein.

Viele Unternehmen behalten die Nutzung dieser Funktion deshalb bestimmten Personen oder Funktionseinheiten vor (beispielsweise der Pforte, wenn sie etwa in einem Notfall eine Warnung verschicken muss, und der Firmenleitung, wenn es zum Beispiel um Weihnachtsgrüße an alle geht). Solche Beschränkungen sind weder Schikane noch Misstrauen. Sie verhindern im Gegenteil Pannen größerer Art.

Wegducken hilft nicht!

In jedem Fall gilt: Sollte es zu einer Versendungspanne kommen, muss dies sofort dem Vorgesetzten gemeldet werden. Denn nur so kann das Unternehmen seine Meldepflicht gegenüber der Datenschutzaufsicht erfüllen.

Impressum

Redaktion: Peter Brandmann (V.i.S.d.P.)

Externer Datenschutzbeauftragter - Zert. Fachkraft DSGVO

Anschrift:

pb beratung & training

Schnepfenreuther Weg 51

90425 Nürnberg

Telefon: 091 1/3506118

E-Mail: peter.brandmann@pb-beratung-training.de