comdatis
it-consulting

Infobrief Datenschutz

#einfachmittelständischpragmatisch - immer bestens informiert!

Ausgabe 02/2020

Liebe Leserin, lieber Leser,

viele Probleme im Datenschutz lassen sich vermeiden, wenn Unklarheiten beseitigt werden. Ihre aktuelle Ausgabe erklärt deshalb, was im Umgang mit Fotos von Beschäftigten erlaubt ist und was nicht. Ebenso erfahren Sie, wann jemand Kopien Ihres Personalausweises anfertigen darf, ob dies zum Beispiel beim Einchecken in ein Hotel der Fall sein darf oder nicht.

Da die Medien über den Datenschutz bei Windows 10 viel berichten, zeigt Ihnen diese Ausgabe, worauf es bei Windows 10 beim Schutz Ihrer Daten ankommt und was Sie als Nutzer tun sollten. Den Abschluss bilden ein Wissenstest und Hintergrundinformationen zu Cookie-Bannern und zum Online-Tracking. Denn auch hier bestehen oftmals Unklarheiten, welche Folgen Cookies und Nutzerprofile für die eigene Privatsphäre haben können.

Werfen Sie auch einmal einen Blick auf unsere Homepage: https://www.comdatis.de/info.html

Dort finden Sie aktuelle Informationen im Blog, Video-Anleitungen und weitere Informationen.

Beste Grüße aus Ahaus-Alstätte wünscht Ihnen

Markus Olbring

Fotos von Beschäftigten

„Fotos von Beschäftigten? Wenn ein Unternehmer die verwenden will, ist immer eine Einwilligung nötig!“ So hört man es häufig. Wenn es nur so einfach wäre! Lesen Sie, in welchen Situationen tatsächlich eine Einwilligung des Beschäftigten nötig ist, in welchen dagegen nicht.

Bilder sind personenbezogen

Das Bild einer Person enthält personenbezogene Daten, das ist klar. „Näher dran an der Person“ geht kaum, selbst wenn es sich nur um ein Passbild handelt. Wer das Bild einer Person verwenden will, muss deshalb die Regeln des Datenschutzes beachten. Dabei besteht unter Juristen über die Ergebnisse eine fast schon erstaunliche Einigkeit – auch wenn sie sich manchmal auf unterschiedliche Paragrafen stützen. Diese Paragrafen kann man deshalb den Juristen überlassen und sich auf das Ergebnis konzentrieren.

Das Bild im Werksausweis

Kann es sein, dass die Verwendung eines Bildes für die Durchführung des Arbeitsverhältnisses erforderlich ist? Wenn ja, kommt es auf eine Einwilligung des Beschäftigten nicht an. Im Gegenteil: Er ist dann aufgrund des Arbeitsverhältnisses verpflichtet, entweder selbst ein Bild zur Verfügung zu stellen oder zumindest dabei mitzuwirken, ein solches Bild anzufertigen.

Typischer Praxisfall: das Bild für den Werksausweis. Ein Werksausweis ohne Bild kann seine Funktion normalerweise nicht erfüllen. Wenn es Werksausweise gibt, muss sich der Beschäftigte deshalb dafür fotografieren lassen.

Das Bild im Telefonverzeichnis

Damit ist aber zugleich der Zweck beschrieben, dem das Bild ausschließlich dienen darf. Nur weil das Unternehmen es „ohnehin schon einmal hat“, darf das Bild nicht einfach für andere Zwecke genutzt werden. Typischer Praxisfall dafür: Es ist zwar schön, wenn man im Telefonverzeichnis des Unternehmens neben dem Namen ein Bild vorfindet. Wirklich nötig ist das aber nicht. Ein Telefonverzeichnis funktioniert auch ohne Bild.

Deshalb setzt ein Bild im Telefonverzeichnis voraus, dass der Beschäftigte damit einverstanden ist. Das darf ein Unternehmen nicht dadurch umgehen, dass es das Bild für den Werksausweis „einfach so“ auch für das Telefonverzeichnis nutzt. Dazu muss es den Beschäftigten vorher fragen.

Das Bild auf der Internetseite

Man ahnt es: Das trifft erst recht zu, wenn Bilder von Beschäftigten auf die Internetseite des Unternehmens sollen. Auch hier gilt: Natürlich ist es schön, wenn man dort beim Vertriebsteam neben jedem Namen und der zugehörigen Telefonnummer auch ein Bild vorfindet. Erforderlich ist das aber nicht.

Und wie sieht es aus, wenn Beschäftigte an einem Imagefilm des Unternehmens mitwirken sollen? Dazu wird ein Unternehmen schon deshalb niemanden zwingen, weil der „Schauspieler wider Willen“ sonst sicher keine positive Ausstrahlung hat. Unabhängig davon gilt: Ohne Einwilligung geht hier nichts.

Der Nachweis der Einwilligung

Beim Nachweis einer Einwilligung hat sich übrigens kürzlich ein wichtiger Punkt geändert. Bisher musste eine solche Einwilligung zwingend schriftlich erfolgen. Künftig reicht auch die „elektronische Form“, also etwa eine E-Mail. Schließlich geht das Papierzeitalter allmählich zu Ende.

Kopie des Personalausweises – zulässig oder nicht?

Die Frage ist brisanter, als es zunächst scheint: Darf ein Personalausweis kopiert oder eingescannt werden? Inzwischen gibt es dafür sogar eine gesetzliche Regelung, die Sie kennen sollten. Auch sie beantwortet aber nicht alle Fragen.

Zwei Beispiele aus der Praxis

Sie wollen in einem Hotel einchecken. Dass Sie Ihren Personalausweis vorlegen müssen, überrascht Sie nicht. Aber der Hotelangestellte scannt Ihren Ausweis auch noch ein. Ist das in Ordnung?

Und wie sieht es in folgendem Fall aus? Ihr Unternehmen klagt zunehmend über Forderungsausfälle. Der Grund: Einzelne Kunden geben eine Scheinanschrift an, wenn sie auf Kredit kaufen. Die Ware wird an die

Anschrift geliefert, aber nie bezahlt. Anzutreffen ist der Kunde dort später nicht mehr. Daraufhin ordnet Ihr Unternehmen an, die Personalausweise aller Kunden zu kopieren.

Regelung im Personalausweisgesetz

Im Personalausweisgesetz findet sich eine Vorschrift, die solche Fragen eigentlich beantworten sollte. § 20 Absatz 2 dieses Gesetzes regelt Folgendes:

- Den Ausweis darf prinzipiell nur der Ausweisinhaber selbst ablichten.
- Andere Personen dürfen ihn nur mit Zustimmung des Ausweisinhabers ablichten. Dabei muss die Ablichtung eindeutig und dauerhaft als Kopie erkennbar sein.
- Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben.

Abschluss eines Mobilfunkvertrags

Daraus ergibt sich zunächst einmal sehr klar: Eine Kopie des Personalausweises ist gegen den Willen des Ausweisinhabers nicht zulässig. So weit die Grundregel. Vereinzelt gibt es aber andere gesetzliche Regelungen, die eine Kopie erlauben. Wenn Sie zum Beispiel einen Mobilfunkvertrag abschließen oder einen Telefonanschluss anmelden, darf der Anbieter Ihren Personalausweis kopieren. Das erlaubt § 95 Absatz 4 Satz 3 Telekommunikationsgesetz ausdrücklich.

„Ausweiskontrolle“ als Alternative

Was ist die Alternative, wenn eine Kopie nicht erlaubt ist? Kein Problem stellt es dar, sich den Ausweis lediglich zeigen zu lassen. Dann kann man das Bild vergleichen und sehen, ob der angebliche Name stimmt. Auch die Anschrift ist im Personalausweis enthalten. Alles Angaben, die im Geschäftsleben außerordentlich nützlich sind, wenn man die Identität eines Vertragspartners feststellen will.

Notieren von Angaben aus dem Personalausweis

Darf man diese Angaben notieren? Dazu vertreten die Aufsichtsbehörden für den Datenschutz folgende Position:

- Notiert werden dürfen alle Daten, die für das Vertragsverhältnis notwendig sind.
- Hierzu zählt alles, was für die Identifikation ausreicht.
- Im Regelfall sind dies der Vorname, der Nachname, die Adresse und gegebenenfalls die Gültigkeitsdauer.

Seriennummer und Zugangsnummer

Datenschutzrechtlich nicht zulässig ist hingegen das Notieren der Personalausweisnummern (Seriennummer, Zugangsnummer). Diese Daten sind nicht erforderlich, um den Vertragspartner sicher identifizieren zu können.

Die Seriennummer eines Personalausweises besteht aus neun Stellen. Eine Stelle ist dabei normalerweise ein Buchstabe, die anderen acht Stellen sind Ziffern. Beispiel: T22000129. Die Zugangsnummer besteht dagegen aus sechs Stellen. Dabei finden nur Ziffern Verwendung. Beispiel: 938568. Die Zugangsnummer braucht man, wenn man bestimmte elektronische Behördenleistungen nutzen will.

Personenkennzeichen im Ausweis? Fehlanzeige!

Die beiden Beispiele für Seriennummer bzw. Zugangsnummer zeigen, dass der Normalbürger damit tatsächlich nichts anfangen kann. Anders als manche glauben, handelt es sich bei der Seriennummer auch nicht um ein Personenkennzeichen. Beantragen Sie etwa einen neuen Ausweis, weil der alte

Ausweis abgelaufen ist, haben beide Ausweise unterschiedliche Seriennummern.

Personalausweis als Pfand?

Es kommt vor, dass ein Unternehmen sich zum Beispiel bei der Vermietung eines Fahrrads den Ausweis als Pfand geben lässt. Das soll sicherstellen, dass der Entleiher den entliehenen Gegenstand wieder ordnungsgemäß zurückgibt. Diese Vorgehensweise ist jedoch unzulässig.

Der Grund: Während der Hinterlegung sind alle Ausweisdaten ungeschützt sichtbar. Ein Missbrauch ist deshalb denkbar. Daher verbietet § 1 Abs. 1 Satz 3 Personalausweisgesetz, vom Ausweisinhaber zu verlangen, dass er seinen Ausweis hinterlegt.

Sinnvolle Alternativen

Wie kann sich ein Unternehmen dann schützen, wenn es zum Beispiel etwas verleiht? Alternativen wären beispielsweise die Hinterlegung eines Geldbetrags oder eines halbwegs wertvollen Gegenstands (etwa einer Uhr).

Auch hier: Notieren von Angaben zulässig

Kein Problem ist es auch hier, sich den Ausweis zeigen zu lassen und dann den Vornamen, den Nachnamen, die Adresse und auf Wunsch auch die Gültigkeitsdauer des Ausweises zu notieren. Eine Kopie des Ausweises bleibt aber in einem solchen Fall verboten.

Windows 10 und der Datenschutz

Die Aufsichtsbehörden für den Datenschutz haben ausführliche Hinweise zum Microsoft-Betriebssystem Windows 10 veröffentlicht . Warum ist Windows 10 im Fokus der Datenschützer, und worauf sollten Sie als Anwender achten?

Hohe Relevanz durch weite Verbreitung

Es gibt mehrere Betriebssysteme, die auf einem Desktop-PC oder Notebook zum Einsatz kommen können. Trotzdem sind es meistens die Microsoft-Betriebssysteme, die für Schlagzeilen sorgen, wenn es um Fragen der Sicherheit und des Datenschutzes geht.

Dafür gibt es einen einfachen Grund: Die Microsoft-Betriebssysteme sind die Marktführer. Das neue Betriebssystem Windows 10 ist bereits auf vielen Rechnern im Einsatz, und wer sich einen neuen Bürorechner oder einen neuen Laptop kauft, hat in den meisten Fällen gleich Windows 10 an Bord. Die Folge: Mehr als ein Drittel der Computernutzer weltweit setzt Windows 10 ein, Tendenz steigend.

Ist etwas weit verbreitet, steigt das Interesse der möglichen Angreifer. Sicherheitslücken bei Windows 10 sind also vielversprechender für Datendiebe als bei kaum installierten Betriebssystemen. Auch Lücken im Datenschutz können massivere Auswirkungen haben. Denn die Zahl der möglicherweise betroffenen Nutzer ist deutlich höher.

Datenschützer und Sicherheitsbehörden prüfen Windows 10

Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch die Aufsichtsbehörden für den Datenschutz haben sich das neue Microsoft-Betriebssystem genauer angesehen, damit sich die

möglichen Risiken des Einsatzes besser bewerten und Gegenmaßnahmen finden lassen.

Das wesentliche Problem bei Windows 10 ist, dass das Betriebssystem umfangreiche System- und Nutzungsinformationen an Microsoft sendet. Die Erfassung und Übertragung von Telemetriedaten durch Windows zu unterbinden, ist technisch zwar möglich, für Anwender aber nur schwer umzusetzen, so das Ergebnis einer Untersuchung des BSI.

Bei den erhobenen Daten handelt es sich um unterschiedliche Informationen wie zum Beispiel

- Daten über die Nutzung des Computers unter Windows 10 und der an ihn angeschlossenen Geräte,
- Daten über die Performance des Systems,
- Daten, die bei Fehlern wie Programm- oder Systemabstürzen erhoben werden, sowie
- Daten des Windows Defender.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erklärte: „Ziel ist es dabei, den Personenbezug von Nutzungsdaten zu vermindern bzw. deren Übertragung in die Entscheidung der Nutzerinnen und Nutzer zu stellen."

In diesem Zusammenhang hat die DSK ein Prüfschema für das Betriebssystem Windows 10 veröffentlicht. Es gibt Unternehmen die Möglichkeit, die datenschutzrelevanten Fragen im Zusammenhang mit dem Einsatz der Software, der Übertragung von Nutzungs- und Systemdaten sowie der Update-Konfiguration zu bewerten. Dieses Prüfschema sollten Unternehmen nutzen, um über den Einsatz von Windows 10 zu entscheiden und um die Nutzung datenschutzgerecht zu gestalten.

Was Nutzer wissen und tun sollten

Setzt ein Unternehmen nach entsprechender Prüfung Windows 10 ein, kommt es auch auf den Nutzer an, um eine datenschutzkonforme Nutzung dauerhaft möglich zu machen. Zum einen müssen die Nutzer wissen, welche Einstellungen und Konfigurationen bei der eingesetzten Windows-10-Installation im Unternehmen freigegeben sind. Dabei spielt unter anderem die genaue Edition von Windows 10 eine Rolle. Es ist ein Unterschied, ob man zum Beispiel Windows 10 Home, Pro oder Enterprise verwendet.

Ebenso spielt es eine Rolle, welche Apps, die zusammen mit dem Betriebssystem installiert werden, die Mitarbeiter tatsächlich nutzen sollen. Allein unerwünschte Apps durch die Systemadministration im Unternehmen zu deinstallieren, reicht nicht. Denn diese Apps werden bei jeder Aktualisierung von Windows 10 erneut aufgespielt.

Administratoren und Anwender können dauerhaft gefordert sein, um die datenschutzfreundlichen Einstellungen bei einer Windows-10-Installation aufrechtzuerhalten. Da Windows 10 bei der Standardinstallation nicht entsprechend vorkonfiguriert ist, muss dies der Verantwortliche leisten, so die Aufsichtsbehörden für den Datenschutz.

Da sich bislang nicht alle Übermittlungen an Microsoft durch eine entsprechende Konfiguration deaktivieren lassen, müssen daneben weitere technische Maßnahmen zum Einsatz kommen, um eine unbefugte Datenübermittlung zu verhindern. Daneben müssen Unternehmen fortlaufend überwachen, ob anlässlich eines Updates eine erneute Prüfung nötig ist.

Während diese Prüfungen zentral im Unternehmen stattfinden, müssen die einzelnen Anwender darauf achten, dass sie die intern definierten Einstellungen bei Windows 10 nicht ungewollt oder unwissentlich verändern. Windows 10 ist deshalb eine langfristige Aufgabe im Datenschutz und gehört immer wieder auf die Agenda.

Tracking im Internet: Was hat es mit den Cookie-Bannern auf sich?

Viele Internetnutzer stören sich an Zusatzfenstern im Browser, die eine Zustimmung zur Nutzung von Cookies erfragen. Sind solche Cookie-Banner wirklich lästig und unnötig? Wie müssen Webseiten-Betreiber die Nutzer darüber informieren, dass sie ihre Aktivitäten im Internet nachverfolgen möchten?

Störenfried oder Aufklärung?

Mit Texthinweisen oder Bannern auf der Startseite informieren viele Webseiten-Betreiber über den Einsatz sogenannter Cookies. Die Mehrheit der Internetnutzer (55 Prozent) ist von den Bannern genervt, so das Ergebnis einer repräsentativen Umfrage des Digitalverbands Bitkom. Danach kann rund die Hälfte (44 Prozent) nicht nachvollziehen, weswegen Webseiten-Betreiber überhaupt auf Cookies hinweisen müssen. Vier von zehn Internetnutzern (39 Prozent) geben an, dass sie Cookie-Banner nicht beachten. Nur für knapp ein Drittel (31 Prozent) stellen Cookie-Banner eine wichtige Information dar.

Auch die Aufsichtsbehörden für den Datenschutz sind mit vielen Cookie-Bannern unzufrieden. Das liegt aber nicht daran, dass die Aufklärung und die Einwilligung vor dem Einsatz von Cookies und anderen Tracking-Verfahren im Internet unnötig wären. Die vorhandenen Cookie-Banner stören meist nicht nur die Benutzerfreundlichkeit der Dienste, sondern schützen auch nicht vor Tracking, so zum Beispiel das Bayerische Landesamt für Datenschutzaufsicht (BayLDA). Viele der vom BayLDA untersuchten Websites, die Cookie-Banner einsetzen, unterbanden weder die Nachverfolgung der Website-Besucher noch erfüllten sie die Anforderungen an eine zulässige Einwilligung nach der Datenschutz-Grundverordnung (DSGVO).

Online-Tracking ist eine Gefahr für den Datenschutz

Cookie-Banner, die davon ausgehen, dass reines Weitersurfen auf der Website oder Ähnliches eine Einwilligung bedeutet, sind unzulässig. Dasselbe gilt für voraktivierte Kästchen bei Einwilligungserklärungen.

Aus Sicht des Datenschutzes muss der Nutzer informiert einwilligen, wenn Daten über sein Nutzungsverhalten an Dritte weitergegeben werden sollen, wie dies zum Beispiel bei Tracking-Cookies der Fall ist. Andernfalls könnten die Webseiten-Betreiber umfangreiche Nutzerprofile anlegen und auswerten, ohne dass die betroffenen Besucher davon wissen und dem zugestimmt hätten.

Die Folgen eines heimlichen Trackings können schwerwiegend sein, je nachdem, welche Daten gesammelt und von wem zu welchem Zweck ausgewertet werden. So könnte es passieren, dass ein Webseiten-Anbieter die Suchanfragen zu medizinischen Themen protokolliert und einem Nutzer zuordnet, wobei er dann diese Informationen einer Versicherung übermittelt.

Was nun geschehen muss

Website-Betreibende sollten ihre Websites umgehend auf Tracking-Mechanismen überprüfen. Wer Dienste nutzt, die eine Einwilligung erfordern, muss die Einwilligung dafür einholen oder die Dienste entfernen. Dazu gehört auch das weit verbreitete Produkt Google Analytics. Eine Einwilligung ist nur dann wirksam, wenn die Website-Besuchenden der Datenverarbeitung eindeutig und informiert zustimmen. Die einwilligungsbedürftige Datenverarbeitung darf zudem erst dann begonnen werden, nachdem der Nutzer die Einwilligung erteilt hat.

Als Besucher einer Webseite sollte man sich nicht an Cookie-Bannern stören, sondern vielmehr hohe

Anforderungen an einen solchen Hinweis auf geplantes Online-Tracking stellen:

- Informiert der Banner ausreichend über den Zweck und die Empfänger der Daten?
- Ist die Einwilligung nicht schon vorausgefüllt?

Webseiten, die den Ansprüchen des Datenschutzes nicht genügen, sollte man verlassen. Andernfalls könnte man heimlich bei seinen Online-Aktivitäten verfolgt werden.

Quiz: Schützen Sie sich richtig vor Online-Tracking? Machen Sie den Test!

Frage: Cookie-Banner verhindern das heimliche Online-Tracking. Stimmt das?

1. Nein, viele Cookie-Banner informieren unzureichend, erfragen keine Einwilligung und verhindern auch kein Tracking bei fehlender Einwilligung.
2. Ja, diese Banner sind wie eine Barriere gegen das Online-Tracking.

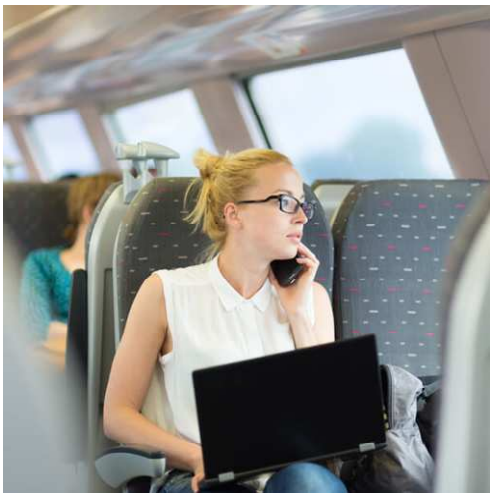
Lösung: Die Antwort 1 ist richtig. Die Aufsichtsbehörden haben viele Cookie-Banner beanstandet, weil sie den Datenschutzvorgaben nicht entsprachen und auch kein Tracking verhinderten, wenn der Webseitenbesucher nicht zugestimmt hat.

Frage: Online-Tracking dient nur der Optimierung einer Webseite, es ist also harmlos. Stimmt das?

1. Ja, die Webseitenbetreiber wollen nur wissen, ob es Probleme mit ihren Internetseiten gibt.
2. Nein, viele Tracking-Daten werden an Dritte übermittelt, die sie für Nutzerprofile verwenden, um personalisierte Online-Werbung auszuspielen.

Lösung: Die Antwort 2 ist richtig. Tracking-Daten können zu sehr genauen Nutzerprofilen führen, die tiefe Einblicke in das Verhalten und die Vorstellungen einer Person erlauben. Denkbar sind Auswertungen, die zum Beispiel das Wahlverhalten vorhersagen oder auf bestimmte Krankheiten schließen lassen. Das Online-Verhalten einer Person kann durchleuchtet und zu Werbezwecken oder sogar zu kriminellen Zwecken missbraucht werden.

Spielregeln für den Umgang mit Datenpannen



Eine Verletzung des Datenschutzes „beichten“ zu müssen, ist immer unangenehm. Jeder weiß, dass es Folgen haben kann, im schlimmsten Fall auch arbeitsrechtliche. Deshalb schweigen manche lieber. Doch Vorsicht! Seit 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO). Nun kann das Verschweigen einer Datenpanne alles noch viel schlimmer machen.

Der verschwundene Laptop

Ein Laptop mit Kundendaten ist weg. Wahrscheinlich blieb er vor ein paar Tagen schlicht im Zug liegen. Das Gerät ist schon fünf Jahre alt und wurde nur noch ausnahmsweise benutzt. Also vermisst es niemand wirklich. Und die Kundendaten sind im EDV-System natürlich noch vorhanden. Da wird auch niemand misstrauisch. Also lieber mal einfach nichts sagen nach dem Motto

„Wird schon gut gehen“? Seit 25. Mai 2018 kann diese Taktik richtig übel enden.

Meldepflicht des Unternehmens ...

Schon vor der Datenschutz-Grundverordnung waren Unternehmen verpflichtet, bestimmte Datenpannen der Datenschutzaufsicht zu melden. Ausgangspunktwar dabei, dass Daten unbefugt übermittelt wurden. Das bedeutet vereinfacht gesagt, dass sie zu Unrecht in die Hände von Außenstehenden gelangt sind. Das allein reichte aber nicht, um eine Meldepflicht entstehen zu lassen. Vielmehr musste noch hinzukommen, dass „schwerwiegende Beeinträchtigungen“ für die Rechte der Personen drohen, um deren Daten es geht.

... bisher oft nur Theorie

Diese Einschränkung führte bisher dazu, dass im Ergebnis oft keine Meldepflicht besteht. Beispiel: Ein Laptop geht verloren. Die Daten auf dem Laptop sind jedoch nach dem Stand der Technik verschlüsselt. Dann kann man davon ausgehen, dass keine schwerwiegenden Beeinträchtigungen drohen. Folge: Eine Meldepflicht entstand im Ergebnis nicht.

Jetzt sieht es anders aus

Die Regelungen der DSGVO für die Meldepflicht sehen anders aus. Sie kennen eine solche Einschränkung nicht. Vielmehr muss ein Unternehmen nun jede „Verletzung des Schutzes personenbezogener Daten“ der Datenschutzaufsicht melden.

Diese Meldepflicht ist in keiner Weise eingeschränkt. Das bedeutet: Der Verlust eines Laptops mit personenbezogenen Daten muss auch dann gemeldet werden, wenn wahrscheinlich alles ausreichend verschlüsselt war.

Meldefrist: 72 Stunden

Das Brisante dabei: Bei der Meldung an die Datenschutzaufsicht ist eine Frist von 72 Stunden zu beachten. Wird sie grundlos überschritten, droht dem Unternehmen schon deshalb ein Bußgeld. Ausreden von der Art „Unser Mitarbeiter hat uns die Panne intern nicht verraten“ gelten dabei nicht. Die Antwort darauf wäre: „Dann bringen Sie Ihren Mitarbeitern eben bei, dass Datenpannen gleich zu melden sind.“

Online-Formulare in Vorbereitung

In der Praxis wird es darauf hinauslaufen, dass eine Meldung an die Datenschutzaufsicht künftig relativ häufig notwendig ist. Die ersten Aufsichtsbehörden (etwa das Bayerische Landesamt für Datenschutzaufsicht) stellen dafür schon Online-Formulare bereit.

Ausnahme: Benachrichtigung der Betroffenen

Ob den Betroffenen, um deren Daten es geht, „etwas passieren“ kann, spielt bei der Meldepflicht keine Rolle. Dieser Aspekt wird erst wichtig, wenn es um die Benachrichtigung der Betroffenen geht. Sie ist gesondert geregelt (Art. 34 DSGVO). Die Betroffenen müssen nur dann benachrichtigt werden, wenn ihnen „voraussichtlich ein hohes Risiko droht“.

Am Beispiel des verschlüsselten Laptops wird wieder deutlich, was das bedeutet: Sind die Daten auf dem Laptop nach dem Stand der Technik verschlüsselt, droht kein hohes Risiko, wenn er Unbefugten in die Hände gerät. Die Folge: Die Betroffenen müssen nicht benachrichtigt werden.

Neue Spielregeln im Überblick

Die neuen Spielregeln, die seit 25. Mai 2018 gelten, lassen sich so zusammenfassen:

- Jeder Mitarbeiter, dem eine Datenpanne unterläuft, muss möglichst sofort seine Vorgesetzten einschalten.
- Nur so lässt sich vermeiden, dass dem Unternehmen ein möglicherweise teures Bußgeldverfahren droht.
- Für die Meldung gilt eine Frist von 72 Stunden. Sie lässt sich nur einhalten, wenn jeder Mitarbeiter Pannen sofort intern meldet.
- Eine Meldung an die Datenschutzaufsicht hat für sich allein noch keine negativen Konsequenzen. Es kann aber natürlich vorkommen, dass die Datenschutzaufsicht genauer nachfragt, was eigentlich genau passiert ist.
- Eine Meldung an die Datenschutzaufsicht führt nicht automatisch dazu, dass die Betroffenen über die Datenpanne benachrichtigt werden. Eine solche Benachrichtigung der Betroffenen ist an relativ enge Voraussetzungen geknüpft.

Impressum

Redaktion:

Markus Olbring

Anschrift:

comdatis it-consulting GmbH & Co. KG

Deventer Weg 8, 48683 Ahaus

Telefon: 02567-82900-00

Mail: info@comdatis.de

Datenschutzinformationen: https://www.comdatis.de/agb.html

Rechtliche Informationen: https://www.comdatis.de/impressum.html