Newsletter Datenschutz

konzept 17

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

was hat das mit Datenschutz zu tun? Diese Frage haben Sie sich vielleicht schon gestellt, wenn Datenschützer in den Medien zu Wort kamen. Tatsächlich betrifft Datenschutz weit mehr, als man denkt.
Unsere neue Ausgabe erinnert etwa an die IT-Ausfälle vor wenigen Monaten, bei denen auch der Datenschutz betroffen war. Warum das so war, erfahren Sie im ersten Beitrag.
Auch die stark diskutierte Künstliche Intelligenz (KI) hat Berührungspunkte mit dem Datenschutz, etwa bei der Datensammlung für das Training. Lesen Sie dazu mehr und testen Sie Ihr Wissen mit unseren Quiz-Fragen.
Es gibt zudem Situationen, in denen man meint, die Datenschutz-Grundverordnung (DSGVO) spiele keine Rolle – etwa bei der „Haushaltsausnahme". Wo diese gilt und wo nicht, erfahren Sie ebenfalls in dieser Ausgabe.
Nicht zuletzt bietet der Datenschutz praktische Vorteile, wie das „Recht auf Kopie" beim Auskunftsanspruch. Was es damit auf sich hat, lesen Sie jetzt.

Ihr Frank Berns, Datenschutzbeauftragter

Impressum
Redaktion: Frank Berns,
Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

Globale IT-Ausfälle: Auch ein Fall für den Datenschutz

Weltweit ist es im Juli 2024 zu IT-Ausfällen gekommen. Auch in Deutschland gab es viele betroffene Unternehmen. Was dabei nicht vergessen werden sollte: Ein IT-Ausfall ist oftmals zugleich eine Datenschutz-Panne

Wenn Computer nicht mehr hochfahren

Es gehört zu den Grundlagen der IT-Sicherheit, dass alle Systeme und Programme regelmäßig aktualisiert werden müssen. Das gilt insbesondere für Lösungen im Bereich Cybersicherheit, denn nur wenn diese auf dem aktuellen Stand sind, gibt es die Möglichkeit, neue Bedrohungen zu erkennen. Wenn aber die Updates und damit die Aktualisierungen und Fehlerbehebungen für die IT nicht gut genug getestet wurden, kann die Installation der Updates zu Problemen führen. Je nach Art der Anwendung und nach dem Umfang der Systemberechtigungen können unerwünschte Reaktionen, stockende Programmabläufe, aber auch weitreichende Störungen und IT-Ausfälle die Folge sein.

Im Juli 2024 passierte genau das: Ein fehlerhaftes Update einer IT-Sicherheitslösung führte dazu, dass die betroffenen Windows-Rechner nach der Installation den eingeleiteten Neustart nicht mehr beendeten. Die Computer kamen nicht zurück in den produktiven Zustand, sondern sie zeigten nur noch einen blauen Bildschirm, in der IT auch „Blue Screen of Death" genannt. Nichts ging mehr bei über 8,5 Millionen Geräten weltweit.

Steht die IT, sind die Daten nicht mehr im Zugriff

Zahlreiche Unternehmen hatten mit Folgewirkungen der Störungen zu kämpfen, so das Bundesamt für Sicherheit in der Informationstechnik (BSI). Viele unternehmerische Prozesse und Abläufe waren durch den Ausfall der Computersysteme oder einzelner Anwendungen gestört.

Was aber bedeutet das für den Datenschutz? Spielt der in einer solchen IT-Krise überhaupt eine Rolle?

Allerdings! Nicht nur die IT-Sicherheit, sondern auch der Datenschutz verlangt neben der Vertraulichkeit und Unveränderlichkeit (Integrität) der Daten die Verfügbarkeit der Daten und die Belastbarkeit der Systeme. Nicht zuletzt verlangt die DSGVO die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Angewandter Datenschutz hilft bei IT-Ausfällen

Wenn es also zu IT-Störungen und Ausfällen kommt, dann wird in den meisten Fällen auch eine mögliche Verletzung des Datenschutzes vorliegen. Auf den ersten Blick scheint diese Feststellung nicht hilfreich zu sein, denn wenn Unternehmen damit kämpfen, ihre Systeme wieder zum Laufen zu bringen, bereitet der Hinweis auf eine zusätzliche Datenpanne noch weiteres Kopfzerbrechen. Doch es ist wichtig, solch umfassende IT-Ausfälle zum Anlass zu nehmen, um sich klar zu machen, dass die Maßnahmen für den Datenschutz mehr bewirken können. Ein wirksames Datenschutzkonzept bietet Maßnahmen, die der IT und dem Unternehmen grundsätzlich helfen, nicht nur der „reinen" Umsetzung der DSGVO. Wenn also der Datenschutz sichere sowie verfügbare Backups fordert und Tests einer schnellen Wiederherstellung der Systeme im Störungsfall, ist dies eine Forderung, die der ganzen IT und damit auch der Funktionstüchtigkeit der digitalen Abläufe und Verfahren im Unternehmen dient. Es zeigt sich: Datenschutz ist kein Selbstzweck und bietet mehr als den Schutz der Privatsphäre!

„Haushaltsausnahme" von der DSGVO

„Für mich privat kann ich machen, was ich will!" Dieser Satz hat einen wahren Kern – auch was die Geltung der DSGVO betrifft. Aber Vorsicht ist geboten, vor allem wenn Berufliches und Privates sich eng berühren.

Es geht um die Anwendbarkeit der DSGVO

Der Begriff „Haushaltsausnahme" ist eine Kurzformel für bestimmte Ausnahmen vom Anwendungsbereich der DSGVO. Im Text der DSGVO sucht man den Begriff vergebens. Dort ist jedoch Folgendes geregelt: Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiäre Tätigkeiten." (Siehe Art. 2 Abs. 2 Buchstabe c DSGVO). Hierfür hat sich als Schlagwort der Begriff „Haushaltsausnahme" eingebürgert. Sogar der Europäische Gerichtshof (EuGH) verwendet ihn immer wieder.

Der Gegensatz zur Haushaltsausnahme ist klar

Den Gegensatz zu „persönlichen oder familiären Tätigkeiten" bilden „berufliche oder wirtschaftliche Tätigkeiten". So erläutert es Erwägungsgrund 18 Satz 1 zur DSGVO. Der europäische Gesetzgeber geht also davon aus, dass berufliche und persönliche Tätigkeiten ein Gegensatzpaar darstellen. Eine berufliche oder wirtschaftliche Beziehung zwischen Menschen ist aus seiner Sicht etwas anderes als eine persönliche Beziehung.

Für berufliche Dinge gilt die DSGVO voll

Auf dieser Basis gilt: Was sich im beruflichen Bereich abspielt, fällt niemals unter die „Haushaltsausnahme". Für die Verarbeitung von personenbezogenen Daten im beruflichen Bereich gelten deshalb immer die Spielregeln der DSGVO. Notwendig ist daher eine Rechtsgrundlage für die Verarbeitung der Daten wie etwa ein Vertrag. Und selbstverständlich können sich betroffene Personen auf ihre Rechte berufen, beispielsweise auf das Recht auf Auskunft über ihre personenbezogenen Daten.

Das reale Leben ist sehr facettenreich

Die Realität des Lebens ist jedoch oft deutlich bunter, als es sich der Gesetzgeber vorstellen kann. Hierzu ein Beispiel: Kollegen tauschen sich über WhatsApp immer wieder privat aus. Dienstliche Dinge bleiben dabei außen vor. Das ändert sich allerdings, als es unerwartet viele Krankheitsfälle im Unternehmen gibt. Um alles am Laufen zu halten, schicken sich Kollegen per WhatsApp Anschriften von Kunden zu oder auch das Foto eines Vertrages.

Der private Bereich ist rasch verlassen

Es liegt auf der Hand, dass in solchen Fällen der private Bereich verlassen ist. Die „Haushaltsausnahme" gilt in derartigen Situationen konsequenterweise nicht mehr. Genauer gesagt, gilt sie für den dienstlichen Teil der Kommunikation nicht mehr. Im Ernstfall müssen die Kommunikationspartner dann sehen, wie sie den dienstlichen und den privaten Teil ihres Austausches voneinander trennen. Das wird vor allem dann relevant, wenn ein betroffener Kunde einen Auskunftsanspruch gelten macht.

Das Internet ist ein öffentlicher Ort

Fotos, etwa von einem gemeinsamen Team-Ausflug, sind eine schöne Sache. Und es ist auch kein Problem, sie im Team auszutauschen, etwa in einer WhatsApp-Gruppe, die das Team privat gebildet hat. Das ist eine Aktivität, die unter die „Haushaltsausnahme“ fällt. Anders sieht es aus, wenn ein Gruppenmitglied „hinter dem Rücken der anderen“ ein paar Fotos auf seine öffentliche Facebook-Seite stellt. Es gilt die Faustregel: Wenn jemand Bilder von zunächst rein privaten Aktivitäten öffentlich ausbreitet, ist das keine Privatangelegenheit mehr. Daher gilt die „Haushaltsausnahme“ hierfür nicht.

Eine enge Auslegung der Ausnahme ist sinnvoll

Auf den Satz „Ausnahmen sind eng auszulegen“, reagieren manche Menschen eher etwas allergisch. Der EuGH verwendet diese Formel allerdings immer wieder. Und das aus gutem Grund. Denn der Sinn der „Haushaltsausnahme“ besteht darin, dass sich die DSGVO nicht in rein private Vorgänge einmischen soll. Wer privat Tagebuch führt oder – ob digital oder analog – ein rein privates Fotoalbum hat, soll nicht über die DSGVO nachdenken müssen. Denn die Interessen anderer Menschen berührt das im Normalfall in keiner Weise.

„Tricksereien“ sollte man bleiben lassen

Umgekehrt gilt logischerweise: Sobald Interessen anderer Menschen in relevanter Weise berührt werden, ist kein Platz mehr für die „Haushaltsausnahme“. Dabei muss es in keiner Weise um schlimme Dinge gehen. Dies zeigt das Beispiel der Kundendaten, die ein Kollege einem anderen privat per WhatsApp schickt. Das soll gewiss nur dafür sorgen, dass der Kunde seine Lieferung trotz diverser Krankheitsfälle im Unternehmen erhält. Es verlässt aber doch den Bereich rein privater Aktivitäten. Und das sollte man einfach im Hinterkopf haben.

Das Recht auf eine Kopie – ein Rätsel?

Betroffene Personen haben ein „Recht auf Erhalt einer Kopie“ ihrer Daten. Das scheint einfach und klar. Die Tücken dieses Anspruchs zeigen sich jedoch jeden Tag in der Praxis.

Ausgangspunkt ist Art. 15 DSGVO

Betroffene Personen haben ein Recht auf Auskunft über die personenbezogenen Daten, die sie betreffen. So legt es Art. 15 Abs. 1 DSGVO fest. Der Anspruch richtet sich gegen den Verantwortlichen, also etwa gegen ein Unternehmen, das Daten von Kunden verarbeitet. Weiter legt die DSGVO fest: „Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.“ (Art. 15 Abs. 3 Satz 1 DSGVO).

Es geht um einen einheitlichen Anspruch

Lange war umstritten, ob die DSGVO hier zwei Ansprüche nebeneinander festlegt. Das eine wäre der Anspruch auf Auskunft über die personenbezogenen Daten (Art. 15 Abs. 1 DSGVO), das andere der Anspruch auf eine Kopie dieser Daten (Art. 15 Abs. 3 DSGVO). Aus der Sicht des EuGH geht es hier aber nur um zwei Facetten ein- und desselben Anspruchs. Er sieht das Zusammenspiel der beiden Facetten so:

- Betroffene Personen haben Anspruch auf Auskunft über ihre personenbezogenen Daten.
- Es geht dabei aber in der Regel nur um den Inhalt dieser Daten, nicht um ihre äußere Form.
- Ein Anspruch auf eine exakte Kopie („1:1“) besteht nur dann, wenn das für das Verständnis des Inhalts notwendig ist.

Typisches Beispiel ist das „leere Leerfeld“

Jemand füllt einen Patienten-Fragebogen aus. In das Feld „bekannte Herzerkrankungen“ schreibt er schlicht nichts hinein. Felder zu anderen bekannten Erkrankungen füllt er dagegen aus. Er verlangt Auskunft über die gespeicherten Daten. Eine bloße Auflistung aller Daten, die er aktiv in den Fragebogen hineingeschrieben hat, gäbe hier kein vollständiges Bild. Die Information, dass er zu Herzerkrankungen nichts hineingeschrieben hat, ist vielmehr ganz wesentlich. Deshalb hat er in diesem Fall Anspruch auf eine Kopie des Fragebogens. Nur einer solchen Kopie lässt sich entnehmen, dass im Feld „Herzerkrankungen“ gerade nichts stand.

Auch für „normale Unternehmen“ ist das alles wichtig

Die eben erörterten Dinge verringern den Aufwand, wenn ein Unternehmen Auskunft erteilen muss. Angenommen, ein Kunde füllt bei jeder Online-Bestellung auf der Webseite des Unternehmens ein Bestellformular aus. Alle Bestellformulare werden gespeichert. Zugleich werden alle Angaben aus den Formularen automatisch in ein Kundenkonto übertragen.

Der Kunde verlangt Auskunft über seine personenbezogenen Daten. Es macht einen erheblichen Unterschied, ob ein Ausdruck des Kundenkontos mit allen Daten genügt oder ob jedes einzelne Bestellformular ausgedruckt werden muss. Der Ausdruck des Kundenkontos genügt hier. Eine Kopie der einzelnen Bestellformulare kann der Kunde dagegen nicht verlangen.

Der Personenbezug ist wesentlich

Aus verschiedenen rechtlichen Gründen müssen Unternehmen ihren Kunden zahlreiche Informationen zur Verfügung stellen. Besonders trifft das Versicherungsunternehmen. Der eigentliche Versicherungsvertrag besteht oft nur aus einer oder zwei Seiten. Als Anlage kommen dann allerdings Versicherungsbedingungen von meist vielen Dutzend Seiten dazu. Diese Versicherungsbedingungen sind nicht individuell ausgestaltet. Vielmehr erhält jeder Kunde exakt dieselben Textdokumente. Als personenbezogen sehen die Gerichte in solchen Fällen nur den eigentlichen Vertragstext an. Die zusätzlichen Textdokumente haben dagegen keinen Personenbezug.

Das blockiert schikanöse Auskunftsforderungen

Für Versicherungsunternehmen ist dieser Aspekt sehr wichtig. Sollte ein Kunde Auskunft über seine personenbezogenen Daten fordern, genügt in der Regel eine Zusammenstellung seiner Daten aus dem Vertrag selbst und eine Zusammenstellung seiner Daten aus dem Versicherungsantrag. Daten über Zahlungsvorgänge und dergleichen können natürlich noch hinzukommen. Wichtiger ist jedoch, was das Unternehmen nicht zur Verfügung stellen muss:

- Eine exakte Kopie des Versicherungsvertrags ist ebenso wenig erforderlich wie eine exakte Kopie des Versicherungsantrags.
- Eine Kopie des Versicherungsantrags ist nur notwendig, wenn er „leere Felder“ enthält. Denn das ist eine wesentliche Information.
- Den Inhalt der Versicherungsbedingungen muss die Versicherung dagegen nicht zur Verfügung stellen. Denn diese Bedingungen sind nicht personenbezogen.

Es liegt auf der Hand, dass diese Aspekte den Aufwand für das Unternehmen erheblich verringern.

Der Datenhunger der Künstlichen Intelligenz

Künstliche Intelligenz (KI) muss zuerst trainiert werden, um den Anwendern Vorteile bringen zu können. Basis eines KI-Trainings sind geeignete Daten, aus denen die KI-Modelle lernen können. Viele KI-Projekte machen aber den Fehler, auf möglichst viele Daten zuzugreifen.

Darum ist KI ein wichtiges Thema für den Datenschutz

KI wird zu den wichtigsten technologischen Entwicklungen der nächsten Jahre oder sogar Jahrzehnte gezählt. Sowohl im beruflichen wie im privaten Bereich hat KI bereits Einzug gehalten, wie zum Beispiel die hohe Verbreitung der KI-Anwendung ChatGPT zeigt.

Es gehört zu den Aufgaben des Datenschutzes, sich auch mit solch neuen Technologien zu befassen, um mögliche Auswirkungen auf personenbezogene Daten frühzeitig erkennen zu können.

Die Landesdatenschutzbeauftragte von Nordrhein-Westfalen (NRW) beispielsweise erklärte, der Knackpunkt sei vor allem der Datenhunger von KI. Datenschutz setze auf das Prinzip der Datensparsamkeit oder Datenminimierung, während KI Datenhunger habe. Grundsätzlich dürften personenbezogene Daten aber nur dann für KI genutzt werden, wenn es gesetzlich erlaubt – also legitim – ist oder die betroffene Person ihre Einwilligung erteilt hat.

Beispiel: Der Meta-Konzern will seine KI trainieren

Der Meta-Konzern, der unter anderem Facebook anbietet, informierte im Mai 2024 Anwenderinnen und Anwender über die geplante Nutzung personenbezogener Daten aus Facebook, Instagram und Threads für die Entwicklung und Verbesserung seiner KI-Dienste. Meta hatte dabei auch auf die Möglichkeit hingewiesen, hiergegen Widerspruch einzulegen. Andernfalls sollten dann Beiträge, Fotos und Bildunterschriften auf Facebook und Instagram zum Training der KI-Dienste von Meta verwendet werden.

Meta hatte sich auf das sogenannte „berechtigte Interesse“ daran berufen, seine KI-Dienste weiterzuentwickeln. Da die EU-Datenschutzbehörden bezweifeln, dass dieses Vorgehen datenschutzkonform ist, ist Meta einer Aufforderung durch die federführende irische Datenschutzaufsicht in der EU nachgekommen und hat bis auf Weiteres das Training seiner KI-Modelle mit Daten aus der EU gestoppt, wie die Landesdatenschutzbeauftragte von NRW berichtete.

Das KI-Training braucht Grenzen

Es zeigt sich: Das Training einer KI-Anwendung kann personenbezogene Daten betreffen und benötigt dafür dann eine entsprechende Rechtsgrundlage. Der Datenschutz verlangt, dass personenbezogene Daten sparsam und zweckgebunden eingesetzt werden. Es muss zudem transparent sein, was mit den Daten geschehen soll und welche Auswirkungen die Verarbeitung der personenbezogenen Daten haben kann.

Bevor man also in einem KI-Projekt damit beginnt, die KI zu Trainingszwecken mit Daten zu füttern, müssen die Folgen für den Datenschutz geklärt sein. Insbesondere muss geprüft sein, ob man nicht auf anonyme, pseudonyme oder synthetische Daten ausweichen kann, ob also ein Personenbezug der Daten wirklich für den Zweck der KI notwendig ist. Das wird in aller Regel nicht der Fall sein.

Wenn aber doch personenbezogene Daten für das KI-Training benötigt werden sollten, muss geklärt werden, ob es eine Rechtsgrundlage für die Verwendung personenbezogener Trainingsdaten gibt.

Bei besonderen personenbezogenen Daten wie Gesundheitsdaten ist in aller Regel eine Einwilligung der betroffenen Personen notwendig.

Das Training einer KI ist also ein Ernstfall für den Datenschutz!

Wissen Sie, warum Künstliche Intelligenz (KI) und KI-Training ein Thema für den Datenschutz sind?

Frage: Wenn man mit einem KI-Projekt startet, ist die KI-Anwendung bereits fertig und einsatzbereit. Stimmt das?

1. Nein, das Besondere an KI-Anwendungen ist, dass sie lernfähig sind. Um zu dem genauen Anwendungszweck zu passen, wird die KI zuerst entsprechend trainiert.
2. Ja, wie jede professionelle Software sind KI-Anwendungen vor der Nutzung fertig entwickelt und bereit für den Einsatz.

Lösung: Die Antwort 1 ist richtig. Wenn eine KI-Anwendung von einem Anbieter bezogen wird, ist diese zwar als Software oder Service fertiggestellt, oftmals ist die KI auch vortrainiert, man beginnt also nicht bei Null. Doch für die individuelle Nutzung der KI-Anwendung kann die KI in dem Projekt weiterlernen und sich damit immer mehr auf den speziellen Einsatzzweck anpassen. Das KI-Training kann also auch noch im Anwenderunternehmen stattfinden.

Frage: KI lernt von uns Menschen. Deshalb sind personenbezogene Daten für das KI-Training unersetzlich. Stimmt das?

1. Ja, ohne Daten von uns Menschen kann eine KI keine Intelligenz entwickeln, wie wir sie von ihr erhoffen.
2. Nein, KI lernt zwar von uns Menschen, sie benötigt dafür aber nicht zwingend Daten über einzelne Personen. Vielmehr soll eine KI Muster erlernen, wie wir Menschen Entscheidungen fällen.

Lösung: Die Antwort 2. ist richtig. Auch aus anonymisierten Daten oder künstlich erzeugten, synthetischen Daten kann eine KI die Muster erkennen, die sie für das Lernen benötigt. Ein Beispiel: Wenn Ärztinnen und Ärzte Röntgenbildern bestimmte Diagnosen zuordnen, dann kann eine KI neue Röntgenbilder mit bereits klassifizierten Bildern vergleichen und bei entsprechender Ähnlichkeit die Wahrscheinlichkeit für eine bestimmte Diagnose berechnen. Dazu muss die KI aber nicht wissen, von welchen Personen die Röntgenaufnahmen sind.