DataGuard

Whitepaper

Von Marijam Özdemir und Tobias Theelen

DIE TOP 6 DATENSCHUTZFEHLER IN UNTERNEHMEN

EINLEITUNG

Kommt Ihnen dieser Satz bekannt vor?

☐ **„Hiermit akzeptiere ich die Datenschutzerklärung."**

Eine oft gewählte Checkbox unter diversen Formularen im Internet und … überflüssig. Eine Datenschutzerklärung muss nämlich nicht akzeptiert werden, da sie nur eine Informationspflicht erfüllt.

In den drei Jahren seit dem Inkrafttreten der DSGVO gab es viel Panik rund um Themen wie Einwilligungen und die Rechtsgrundlage für Datenverarbeitungsprozesse. Eine Datenschutzerklärung muss jedes Unternehmen auf seiner Website haben, das stimmt. Jedoch müssen Kontakte dieser nicht „zustimmen", um eine Datenverarbeitung zu rechtfertigen. Stattdessen sind ganz andere Einwilligungen notwendig. Doch mehr dazu später.

Immer wieder stolpern wir in unserer Kundenbetreuung über die gleichen Fehler und Fehlinterpretationen rund um Datenschutz, Informationssicherheit und die DSGVO. Die Konsequenzen dieser Irrtümer können ganz unterschiedlich ausfallen – von kleinen Unannehmlichkeiten für Sie oder Ihre Kunden über negative Bewertungen auf Vergleichsportalen bis hin zu teuren Bußgeldern.

Fast jedes Unternehmen tappt an irgendeiner Stelle im Dunkeln. Zu den meisten Fehlern, die wir beobachten, gehören:

1. Fehlversendung von E-Mails
2. Ausufernde CV-Datenbanken von Headhuntern und HR-Abteilungen
3. Falsche oder sinnlose Checkboxen unter Formularen auf der Website
4. Fehlende Mitarbeiterschulung zu Datenschutzthemen
5. Falsche Abgrenzung von Verantwortlichkeit vs. Auftragsverarbeitung
6. Angst vor Aufsichtsbehörden

Glücklicherweise können Sie all diesen Fehlern recht einfach vorbeugen. Der erste Schritt ist dabei – wie immer – die Einsicht. Wir erklären also, über welche Fallstricke viele Unternehmen stolpern und wie es besser geht.

INHALT

FEHLVERSENDUNG VON E-MAILS

DER HINTERGRUND

Der absolute Klassiker unter den Datenschutzverletzungen: die E-Mail mit Empfängern in cc, die da nicht hingehören. Vielleicht denken Sie jetzt: Sowas kann mir nicht passieren! Unsere täglichen Erfahrungen zeigen anderes: Die offene Empfängerliste gehört nach wie vor zu den gängigsten Datenpannen in Unternehmen.

Jeden Tag werden wahrscheinlich Millionen von E-Mails mit Personen in cc (Carbon Copy) versendet. Und in der Regel passiert gar nichts. Die Personen in cc können – genau wie die regulären Empfänger – sehen, an welche E-Mail-Adressen die Nachricht versandt wurde. Zudem ist der gesamte Verlauf einsehbar. Zu Problemen führt das dann, wenn es Empfänger gibt, die …

- die E-Mail-Adressen der anderen Empfänger nicht kennen sollten;
- über den Verlauf an personenbezogene Informationen gelangen, die nicht mit ihnen geteilt werden sollten.

DIE RECHTSLAGE

Solange sich die E-Mail-Adresse einer natürlichen Person zuordnen lässt, gilt sie nach Art. 4 Nr. 1 DSGVO als personenbezogenes Datum. Und dieses darf Dritten nur mit Einwilligung oder einer anderen entsprechenden Rechtsgrundlage zur Verfügung gestellt werden. Wird die E-Mail-Adresse wie im Fall der offenen E-Mail-Liste geteilt, liegt also ein Verstoß gegen den Datenschutz vor.

SO KANN SICH DER FEHLER IN DER PRAXIS ÄUSSERN

Ein Verband möchte all seine Mitglieder und eine Liste von Interessierten über eine gesetzliche Neuerung informieren. Dafür setzt die Verwaltung des Verbands einen kleinen Newsletter auf. Um diesen direkt an alle Empfänger zu verschicken, werden die E-Mail-Adressen von Mitgliedern und Interessierten in das cc-Feld kopiert. So bekommen zwar alle Empfänger das Update,

allerdings werden auch gleich die E-Mail-Adressen aller anderen Mitglieder mitversendet. Das ist ein klarer Verstoß gegen den Schutz personenbezogener Daten im Sinne der Vertraulichkeit.

Ein weiteres Beispiel: Ein Logistik-Unternehmen will seine Umsätze im Q1 2021 ankurbeln und gewährt Neukunden, die noch in Q1 einen Vertrag abschließen, einen Rabatt von 20 %. Eine Vertriebsmitarbeiterin will direkt drei der Unternehmen informieren, mit denen Sie gerade in Verhandlungsgesprächen steckt. Um Zeit zu sparen (denn die ist im Vertrieb bekanntlich immer knapp), sendet sie einfach eine E-Mail an einen der möglichen Neukunden und setzt die anderen in cc. Auch hier werden personenbezogene Daten geteilt. Und noch schlimmer: Die Empfänger erhalten Informationen darüber, dass die anderen Unternehmen sich gerade ebenfalls in Verhandlungsgesprächen befinden.

BUßGELDER

Der sogenannte offene E-Mail-Verteiler hat bereits vor Einführung der DSGVO zu einigen Bußgeldern geführt. Das Bayrische Landesamt für Datenschutz verhängte schon im Jahr 2013 ein Bußgeld von 2.500 EUR gegen ein Unternehmen, da eine Mitarbeiterin eine E-Mail mit einem großen Empfängerkreis in cc versendet hatte. Ähnlich hart traf es einen Merseburger, der Wut-Mails an große Verteiler in cc schickte. Er zahlte knapp 2.500 EUR aus eigener Tasche. Auch die Stadt Konstanz bekleckerte sich 2019 nicht gerade mit Ruhm, als ein städtischer Info-Newsletter an über 350 E-Mail-Adressen rausging. Da es sich um eine öffentliche Stelle handelt, kam es hier jedoch zu keinem Bußgeld.

SO GEHT ES BESSER

Die Lösung für diesen Datenschutz-Fauxpas ist ganz einfach:

1. Statt des cc-Feldes sollte das bcc-Feld direkt darunter genutzt werden. Bcc steht für „Blind Carbon Copy" – die Empfänger dieser Zeile sehen nur den Absender und den Inhalt der E-Mail bzw. des E-Mail-Verlaufs.
2. Vor dem Weiterleiten von E-Mail-Verläufen an weitere Empfänger lohnt sich ein zusätzlicher Check. Sind wirklich alle Informationen in den E-Mails für die neuen Empfänger geeignet?
3. Für Newsletter empfehlen wir die Nutzung dedizierter Tools, die direkt auch andere Datenschutzgrundsätze wie die Einwilligung durch das Double-Opt-In-Verfahren erlauben und speichern sowie „Unsubscribe"-Links zur Abmeldung mitversenden.
4. All das kann nur dann gelingen, wenn Mitarbeiter im Umgang mit personenbezogenen Daten geschult werden. Mehr dazu in Kapitel vier.

AUSUFERNDE CV-DATENBANKEN VON HEADHUNTERN UND HR-ABTEILUNGEN

DER HINTERGRUND

Wäre es nicht praktisch, die Daten aller Bewerber für immer zu speichern? So hätte man für jede offene Stelle gleich einen Haufen an möglichen Kandidaten, die man anschreiben oder anrufen könnte.

Weil diese Vorstellung so verlockend ist, legen sich viele Personalabteilungen und Headhunter tatsächlich ganze Datenbanken voller Lebensläufe und Arbeitszeugnisse an. Rechtens ist das nur leider nicht.

DIE RECHTSLAGE

Lebensläufe, Arbeitszeugnisse und Bewerberakten gehören zweifelsohne zur Kategorie der personenbezogenen Daten. Damit muss sich ihre Verarbeitung und Speicherung auf eine Rechtsgrundlage stützen (Art. 6 DSGVO). Verfällt diese Rechtsgrundlage, sind die Daten zu löschen. Zudem müssen Betroffene (also in diesem Fall Bewerber) u. a. über den Zweck und die Dauer der Datenverarbeitung informiert werden, wie in Art. 13/Art. 14 DSGVO beschrieben.

Art. 6 DSGVO nennt folgende mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten:

- Einwilligung der betroffenen Person
- Erforderlichkeit für die Erfüllung eines Vertrags
- Erforderlichkeit für die Erfüllung einer rechtlichen Verpflichtung
- Erforderlichkeit zum Schutz lebenswichtiger Interessen des Betroffenen
- Erforderlichkeit zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt
- Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen

Als Rechtsgrundlage der Datenverarbeitung im Bewerbungsprozess lässt sich in Deutschland das BDSG zugrunde legen: Gemäß § 26 Abs. 8 S. 2 BDSG in Verbindung mit § 26 Abs. 1 S. 1 BDSG kann abgeleitet werden, dass personenbezogene Daten von Bewerbern für Zwecke des Bewerbungsverfahrens verarbeitet werden dürfen, wenn diese für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich sind.

Sobald also ein Bewerber abgelehnt wurde, dürfen die Bewerbungsunterlagen aufgrund gesetzlicher Fristen noch eine Zeit lang aufbewahrt werden, sind aber nach Verstreichen der gesetzlichen Fristen zu vernichten/zu löschen.

Sollen Daten länger gespeichert werden, so ist dies nur mit Einwilligung der Betroffenen möglich. In jedem Fall ist die Informationspflicht nach Art. 13 (DSGVO) einzuhalten. Dabei müssen Betroffene u. a. über die Datenverarbeitung informiert werden:

- Zwecke der Datenverarbeitung
- Die berechtigten Interessen, auf denen die Rechtmäßigkeit der Datenverarbeitung beruht, sofern dies die Rechtsgrundlage zur Verarbeitung ist
- Informationen zur Übermittlung der Daten in Drittländer
- Die Dauer der Datenverarbeitung
- Hinweis auf Auskunfts-, Beschwerde- und Widerrufsrecht

BUßGELDER

In Deutschland gab es bisher noch keine Bußgelder für die Speicherung von Bewerberdaten über den Bewerbungsprozess hinaus. Eines der höchsten Bußgelder, die bisher verhängt wurden, basierte allerdings auf einem ganz ähnlichen Fall: Die Deutsche Wohnen speicherte die Daten von Mietern und Mietbewerbern ohne Löschkonzept über Jahre hinweg. Die Strafe: satte 14,5 Millionen EUR. Das Problem bei der Speicherung von Mietbewerberdaten ist die fehlende Rechtsgrundlage – so auch im Fall Deutsche Wohnen.

SO GEHT ES BESSER

Zum einen sollten Unternehmen ihren Prozess für Bewerber unter die Lupe nehmen. Werden die Bewerber u. a. bereits über Zweck und Dauer der Datenverarbeitung in Kenntnis gesetzt? Wenn nicht, könnte die E-Mail zur Eingangsbestätigung der Bewerbung entsprechend ergänzt werden. Gibt es ein Löschkonzept für die Daten von Bewerbern oder eine Anfrage für die Einwilligung einer längeren Speicherung – zum Beispiel, um für zukünftige offene Stellen berücksichtigt zu werden?

Viele Recruiter nutzen längst professionelle Netzwerke wie Xing und LinkedIn, um mit Bewerbern in Kontakt zu bleiben. Das hat Vor- und Nachteile. Einerseits wird ein LinkedIn-Profil laufend aktualisiert und die Kontaktaufnahme ist unkompliziert, andererseits gehen die so geknüpften Verbindungen verloren, wenn ein Recruiter das Unternehmen verlässt. In jedem Fall ist die Nutzung von beruflichen Netzwerken aber eine sinnvolle Ergänzung.

FALSCHE UND/ODER SINNLOSE CHECKBOXEN UNTER FORMULAREN AUF DER WEBSITE

DER HINTERGRUND

Der Datenverarbeitung zu Marketingzwecken wird besonders gern die Einwilligung der Betroffenen als Rechtsgrundlage zugrunde gelegt. Das leuchtet ein, da die anderen Rechtsgrundlagen bei Kontakten, die noch keine Kunden sind, meist nicht einschlägig sind. Es werden also fleißig Einwilligungen eingeholt. Sinnvoll sind diese nicht immer – und manchmal werden im Checkboxen-Übereifer die eigentlich wichtigen Informationen vergessen.

DIE RECHTSLAGE

Die DSGVO liefert keinen fertigen Vordruck für die Gestaltung von Checkboxen mit – auch wenn sich viele Unternehmen sicher darüber freuen würden. Allerdings liefert die DSGVO klare Vorgaben dazu, wie Einwilligungen eingeholt werden müssen.

Empfehlenswert ist es, auf dem Formular mindestens folgende Elemente abzubilden:

- Aufklärung über den Zweck der Datenerhebung (Zweckbindungsprinzip gemäß Art. 5 Abs. 1 lit. b DSGVO)
- Hinweis auf die Widerrufbarkeit der Einwilligung
- **Freiwillige** Checkbox zur Einwilligung in die Zusendung von Marketinginformationen und/oder Kontaktaufnahme durch den Vertrieb

Nach Art. 7 DSGVO gehört die Freiwilligkeit zu den Bedingungen für eine rechtsgültige Einwilligung. Der genaue Wortlaut in Art. 7 Abs. 4 DSGVO liest sich wie folgt:

> „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind."

DIESE FEHLER SIND IN DER PRAXIS BESONDERS GÄNGIG

In diesem Beispiel fehlt ein Hinweis zur Möglichkeit des Widerrufs – diesen schreibt die DSGVO allerdings explizit vor. Ebenfalls nicht empfehlenswert ist es, die Checkbox schon vorangekreuzt anzuzeigen. Wichtig ist bei Einwilligungen immer, dass für den Nutzer klar und deutlich erkennbar ist, wozu er zustimmt.

SO GEHT ES BESSER

Wie gesagt: Die DSGVO trifft keine konkreten Aussagen zur Formulierung von Checkboxen. Das gibt Unternehmen den Gestaltungsspielraum, die Einwilligungen an den konkreten Zweck der Datenerhebung und -verarbeitung anzupassen.

Wichtig ist: Trennen Sie das Notwenige vom Optionalen. Fordert ein Website-Besucher eine Checkliste an, die per E-Mail versandt wird, dann führt kein Weg an der Datenverarbeitung für genau diesen Zweck vorbei. Optional allerdings sind weiterführende Marketing-Informationen wie beispielsweise ein Newsletter. Und diese beiden Zwecke sollten nicht miteinander vermischt werden – die Einwilligung zum Newsletter muss freiwillig bleiben.

Eine Einwilligung muss freiwillig geschehen, sollte also nicht im Gegenzug für ein Freebie wie ein E-Book oder Webinar eingefordert werden. Das kann dann zum Beispiel so aussehen:

FEHLENDE MITARBEITERSCHULUNG ZU DATENSCHUTZTHEMEN

DER HINTERGRUND

Egal, wie gut Ihre Serverräume überwacht werden, wie ausgeklügelt Ihre Kryptographie und wie wasserdicht Ihre Auftragsverarbeitungsverträge – wenn Ihre Mitarbeiter nicht aufpassen, sind keine Daten sicher. Die Mitarbeiterschulung gehört laut DSGVO zu den Kernaufgaben eines Datenschutzbeauftragten (DSB).

DIE RECHTSLAGE

Art. 39 DSGVO listet die Aufgaben des DSB. Darunter fällt in lit. b die …

> „[…] Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, **der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter** und der diesbezüglichen Überprüfungen" [Hervorhebung durch die Redaktion]

Wie genau eine solche Schulung nun aussehen sollte, verrät die DSGVO nicht. Auch hier gewährt sie Datenschutzbeauftragten also einen recht großen Spielraum. Ebenfalls ist nicht vorgeschrieben, in welcher Form (also online, persönlich, nur schriftlich …) und in welchen Abständen Schulungen stattfinden sollen. Da sich Verarbeitungsvorgänge jedoch typischerweise laufend verändern, neue Technologien eingesetzt werden und Menschen Gelerntes ohne Wiederholungen schnell wieder vergessen, empfehlen wir bei DataGuard mindestens jährliche Schulungsintervalle.

BEISPIELE FÜR DIE INHALTE EINER MITARBEITERSCHULUNG

Neben den Datenschutzgrundsätzen sollte den Mitarbeitern aufgezeigt werden, welche Rechte die Betroffenen haben. Weitere Inhalte sind die Datenschutzrichtlinie im Unternehmen, Datenschutz bei Verwendung mobiler Endgeräte sowie die Rechtsgrundlagen und wichtige Fachgriffe. Insbesondere ist den Mitarbeitern zu vermitteln, wie sie sich im Fall von Verstößen und Datenschutzverletzungen zu verhalten haben. Die Mitarbeiter, die direkten Kundenkontakt haben, sollten zudem lernen, welche Informationen Sie an Kunden herausgeben können – und unter welchen Voraussetzungen.

Um Schulungen möglichst interessant und kurzweilig zu gestalten, sollten die vorgeschriebenen Themen möglichst nicht in trockener Theorie abgearbeitet werden. Viele Beispiele von Datenschutz im beruflichen Alltag und interaktive Elemente führen dazu, dass die Mitarbeiter die Schulung mit höherer Aufmerksamkeit verfolgen und die Sensibilisierung bei Ausführung der Tätigkeiten Wirkung zeigt.

Damit sich die Mitarbeiter mehr unter den Themen Verzeichnis von Verarbeitungstätigkeiten (VVT), technische und organisatorische Maßnahmen (TOM) und den weiteren Dokumentationspflichten vorstellen können, ist es wichtig, praktische Übungen zu bestimmten Datenverarbeitungsprozessen durchzugehen. Darüber hinaus sollte bei Schulungen ein Fokus auf datenschutzrelevante Aspekte des jeweiligen Mitarbeiters bei der täglichen Arbeit gelegt werden. So wird den Mitarbeitern klar, welche Auswirkungen bestimmte Prozesse haben. Wer nicht nur die Theorie, sondern auch die Praxis kennt, erkennt auch im Alltag Fallstricke und kann auf diese aufmerksam machen und sie umgehen.

INHALTE

- Datenschutzgrundsätze
- Rechtsgrundlagen
- Betroffenenrechte
- Datenschutzrichtlinie des Unternehmens
- BYOD und Verwendung mobiler Endgeräte allgemein
- Verhalten im direkten Kontakt mit Kunden, Partnern, Mitarbeitern, Bewerbern und anderen externen Stakeholdern
- Verhalten im Fall eines Datenschutzverstoßes

FORMAT

- Viele Beispiele aus der Praxis
- Interaktiv
- Am besten auf Abruf online verfügbar
- Rollenspezifische Trainings je nach Tätigkeitsbereich

BUßGELDER

Eines der bekanntesten Bußgelder in Deutschland resultierte aus dem Fehlverhalten eines Service-Mitarbeiters beim Telekommunikationsanbieter 1&1. Die Ex-Freundin eines Kunden rief bei 1&1 an, um an seine neue Handynummer zu gelangen. Dafür musste sie nur Namen und Geburtsdatum des Kunden nennen und bekam die Information bereitwillig mitgeteilt. Der Kunde wurde daraufhin Opfer von Stalking.

In diesem Fall resultierte der Fehler darin, dass keine ordnungsgemäße Identitätsprüfung des Anrufers stattgefunden hat, sodass Daten an einen Dritten herausgegeben wurden. Sowohl die Schulung von Mitarbeitern als auch konkrete Vorgaben von technischen und organisatorischen Maßnahmen hätten diese unbefugte Herausgabe von Daten verhindern können. Die vom Bundesdatenschutzbeauftragten Ulrich Kleber geforderte Strafe von 9,55 Millionen EUR wurde später durch ein Gericht auf 900.000 EUR gekürzt.

SO GEHT ES BESSER

An dieser Stelle können wir kaum auf schamlose Eigenwerbung verzichten. Denn DataGuard hat mit der DataGuard Academy genau die Plattform entwickelt, die Mitarbeiter sowohl in den Grundlagen der DSGVO schult als auch rollenspezifische Trainings zum Beispiel für die IT oder Beschäftige im Homeoffice anbietet.

Aktuell können Sie sich kostenlos für eine Vorschau des Basiskurses anmelden!

Ganz allgemein lässt sich festhalten, dass es für einen internen Datenschutzbeauftragen (DSB) oft schwierig ist, das Team für Trainings zu motivieren. Externe Dienstleister mit Lernplattformen und interaktiven Materialien haben es da leichter.

FALSCHE ABGRENZUNG VON VERANTWORTLICHKEIT UND AUFTRAGSVERARBEITUNG

DER HINTERGRUND

Kundendaten in einem SaaS-CRM (wie Salesforce, Pipedrive oder HubSpot) verwalten, die Lohnbuchhaltung über einen Drittanbieter abwickeln oder einfach nur Newsletter über eine Marketing-Software rausschicken – all das sind Beispiele für Auftragsverarbeitung. Bei dieser werden Daten gemäß den Weisungen des **Verantwortlichen** durch ein anderes Unternehmen (den **Auftragsverarbeiter**) verarbeitet. Immer wieder kommt es dabei zu Unklarheiten, wer welche Pflichten zu erfüllen hat. Muss zum Beispiel ein CRM-Anbieter eine Datenschutzerklärung für seine Kunden erstellen?

DIE RECHTSLAGE

In der DSGVO ist die Auftragsverarbeitung definiert als

> „[…] die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gemäß den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages."

Hier zeigt sich der Knackpunkt: Die Verarbeitung geschieht vollständig auf Weisung des Verantwortlichen. Somit ist dieser auch für die Erstellung einer Datenschutzerklärung zuständig und muss den Auftragsverarbeiter in sein Verzeichnis von Verarbeitungstätigkeiten (VVT) mit aufnehmen. Der Vertrag, der die Zusammenarbeit regelt, nennt sich Auftragsverarbeitungsvertrag (AVV) und wird üblicherweise durch den Auftragsverarbeiter erstellt. Der Auftragsverarbeiter wiederum muss entsprechende Verarbeitungstätigkeiten in einem „Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter" nach Art. 30 Abs. 2 DSGVO listen.

SO GEHT ES BESSER: DIE PFLICHTEN DES VERANTWORTLICHEN UND AUFTRAGSVERARBEITERS VERSTEHEN

DIE PFLICHTEN DES VERANTWORTLICHEN

1. Sicherstellen, dass der AVV wirklich alle Punkte aus Art. 28 der DSGVO abdeckt. Dabei ist insbesondere zu achten auf:
   a. Eine gut definierte Leistungsbeschreibung, aus der genau hervorgeht, welche Teilleistung der Auftragsverarbeiter erbringt
   b. Datenkategorien, die nicht nur oberflächlich, sondern detailliert erklärt sind
   c. Eine Auflistung der Subauftragsverarbeiter des Auftragsverarbeiters und Nachweise über die Prüfung derer Datensicherheit

2. Prüfung der Dokumentation der technischen und organisatorischen Maßnahmen (TOM) des Auftragsverarbeiters. Die TOM zeigen, wie sicher ein Auftragsverarbeiter mit den Daten seiner Kunden umgeht und sind ein wesentlicher Bestandteil von Auftragsverarbeitungsverträgen. Folgende Aspekte sollten z. B. abgedeckt werden:
   a. Verschlüsselungsmaßnahmen
   b. Aufschlüsselungen, wer Zugang zu welchen Daten hat
   c. Informationen zur Serverredundanz und Serversicherheit, um Verfügbarkeiten zu garantieren
   d. Ein Vermerk zur Mandantenfähigkeit Ihrer Lösung
   e. Anmerkungen zu Multi-Faktor-Authentifizierung (zum Beispiel für Admins), falls vorhanden
   f. Dem Zweck der erhobenen Daten, um nachzuweisen, dass nur die für die Bereitstellung des Service notwendige Daten erhoben werden.
   g. Informationen zu Patch-Management und regelmäßigen Updates
   h. Hinweise zum Vorgehen bei der Fernwartung

3. U. u. die Erstellung einer Datenschutz-Folgenabschätzung. Insbesondere beim Einsatz neuer Technologien – wie SaaS-Lösungen – können im Verarbeitungsprozess Risiken für Rechte und Freiheiten Ihrer Kunden und Mitarbeiter entstehen, die eine Datenschutz-Folgenabschätzung erfordern können.

DIE PFLICHTEN DES AUFTRAGSVERARBEITERS

Der Auftragsverarbeiter ist dafür verantwortlich, die Daten gemäß den Weisungen des Verantwortlichen zu verarbeiten. Dabei müssen die Grundsätze der DSGVO eingehalten werden, die auch für andere Unternehmen gelten.
Hinzu kommt eine wichtige und oft vergessene Pflicht: Verstößt eine Weisung des Verantwortlichen gegen die DSGVO, so muss der Auftragsverarbeiter den Verantwortlichen darüber informieren (Art. 28 Abs. 3 DSGVO). Zudem besteht eine Pflicht zur Meldung von Datenschutzverstößen an den Verantwortlichen (Art. 33 Abs. 2 DSGVO).

In unserem Whitepaper für SaaS-Anbieter erklären wir Ihnen, wie Sie nicht nur Ihren notwendigen Pflichten nachkommen, sondern Datenschutz auch zu Ihrem Wettbewerbsvorteil machen können – zum Beispiel, indem Sie Verzögerungen im Vertriebsprozess aufgrund von Datenschutzbedenken vorbeugen.

ANGST VOR AUFSICHTSBEHÖRDEN

DER HINTERGRUND

Es gibt diese Absender auf Briefen, die den Puls in die Höhe schnellen lassen. Niemand freut sich über Post von Finanzamt, Gerichten, der Bank oder eben den Aufsichtsbehörden – denn die Neuigkeiten können eigentlich nur schlecht sein. Meldet sich eine Datenschutzaufsichtsbehörde bei Ihnen, wäre Panik allerdings fehl am Platz. Wir raten: immer cool bleiben. Und vor allen Dingen: kooperieren und Gesprächen mit der Aufsichtsbehörde nicht aus dem Weg gehen.

DIE RECHTSLAGE

Oft kommt es zu Missverständnissen bezüglich der Rolle von Aufsichtsbehörden. Die Aufsichtsbehörde ist keine rechtssprechende Instanz, sondern unterstützt Unternehmen in der Umsetzung von Datenschutzgesetzen und steht bei Fragen zur Verfügung. Daraus folgt auch, dass Empfehlungen der Aufsichtsbehörden zu gewissen Datenschutzthemen nicht Gesetz sind. Ihnen als Unternehmen steht es frei, Datenschutzgesetze anders zu interpretieren, als es die Aufsichtsbehörde tut. Ob das ratsam ist, ist eine andere Frage. Im Zweifelsfall entscheidet ein Gericht.

Neben der beratenden Funktion übernehmen Aufsichtsbehörden auch eine Kontrollfunktion und passen auf, dass Regeln eingehalten werden. Die Zusammenarbeit mit der zuständigen Aufsichtsbehörde gehört nach Art. 39 DSGVO zu den Aufgaben des Datenschutzbeauftragten. Nimmt eine Aufsichtsbehörde also Kontakt mit Ihnen auf, obliegt die offene Kommunikation dem Datenschutzbeauftragter und dem Verantwortlichen.

Gab es in Ihrem Unternehmen einen Datenschutzverstoß, müssen Sie diesen innerhalb von 72 Stunden von sich aus bei der zuständigen Aufsichtsbehörde melden. Bei hohen Risiken müssen Sie zusätzlich die Betroffenen informieren.

Risiko für die persönlichen Rechte und Freiheiten des Betroffenen	Meldepflicht an Aufsichts-behörde notwendig?	Meldepflicht an Betroffene notwendig?
NIEDRIG	JA	NEIN
MITTEL	JA	NEIN
HOCH	JA	JA

PRAXISTIPPS FÜR DEN UMGANG MIT AUFSICHTSBEHÖRDEN

In unserer Rolle als externer DSB sind wir mit den Aufsichtsbehörden im ständigen Austausch und Kontakt. Und wir können jeden beruhigen, der Angst vor ihnen hat. Die Aufsichtsbehörden lassen gut mit sich reden, sind kooperativ und beantworten selbst Rückfragen schnell und freundlich. Fragt eine Aufsichtsbehörde bestimmte Unterlagen an, zählt proaktives und umsichtiges Verhalten. Eine bereitwillige, offene Zusammenarbeit mit der Aufsichtsbehörde kann sich durchaus mildernd auf ein Urteil auswirken.

Bei Datenpannen ist es besonders wichtig, keine Fristen verstreichen zu lassen. Auch, wenn der erste Impuls eine Art Schockstarre sein kann oder der Wunsch, den Vorfall still und heimlich unter den Teppich zu kehren, wäre genau das die falsche Reaktion. Mit einer sofortigen Meldung an die Aufsichtsbehörde beweisen Sie als Unternehmen, dass Sie den Datenschutz ernst nehmen, und Sie schützen sich eher vor hohen Geldstrafen. Wir haben hier einen Reaktionsplan für Sie zusammengestellt.

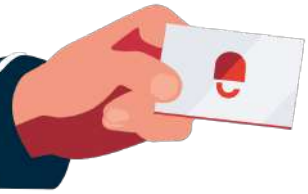
BUßGELDER

Ein sehr bekannter Bußgeldfall in Deutschland betraf das Modeunternehmen H&M. Das Unternehmen soll Mitarbeiter ausgespäht und Inhalte aus informellen Gesprächen – zum Beispiel zu familiären Problemen, Urlaubserlebnissen und Krankheitsbildern – in umfangreichen Mitarbeiterakten gespeichert haben. Kein Kavaliersdelikt also. Doch H&M kooperierte mit der Datenschutzaufsichtsbehörde und bot betroffenen Mitarbeitern proaktiv Schadensersatzleistungen an. Im Gerichtsverfahren wurde dieses Verhalten positiv angerechnet.

ZUSAMMENFASSUNG

Auch, wenn wir uns mit dieser Behauptung weit aus dem Fenster lehnen: Kein Unternehmen macht in Sachen Datenschutz immer alles richtig. Es gibt so einige Hürden und Fallstricke, die zu Fehlern und Missverständnissen führen können. Wichtig ist es, am Ball zu bleiben, den eigenen Datenschutz konstant unter die Lupe zu nehmen und stetig zu verbessern.

Da das komplexe Thema Ihren internen Datenschutzbeauftragten und ihre Teams bisweilen überfordern kann, bieten wir mit unserem „Datenschutz-as-a-Service"-Modell Expertenwissen auf Abruf – kombiniert mit unserer eigenentwickelten Datenschutz-Plattform mit priorisierten To-dos und ständig aktualisierten Datenschutzdokumentationen.



DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Jetzt Termin vereinbaren, um über Ihre Herausforderungen zu sprechen und erste Schritte zu definieren:

Erstgespräch buchen

Weiterführende Ressourcen:

→ **Datenschutzkonformes Cookie-Management & -Tracking**

→ **Übersicht aller Datenschutz-dokumente aus der DSGVO**

→ **On-Demand Webinar: 5 Schritte gegen Datenpannen im Arbeitsalltag**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard