Datenschutz ganz kurz

Was Beschäftigte unbedingt wissen sollten

STIFTUNG DATENSCHUTZ

Einführung

In allen Unternehmen, Praxen, Vereinen und anderen Organisationen werden Informationen über Menschen, zum Beispiel als Beschäftigte, Bewerber*innen, Kund*innen oder Funktionstragende, verarbeitet. Dabei ist es gut, wenn Sie mit den Grundregeln des Datenschutzes sowie den daraus resultierenden wesentlichen Pflichten vertraut sind. Dies betrifft die Mitglieder der Geschäftsleitung ebenso wie Beschäftigte oder Vereinsvorstände und Übungsleitende in allen Bereichen und unabhängig von ihren Anstellungsverhältnissen, auch wenn sie nur gelegentlich mit personenbezogenen Daten arbeiten.

Diese Broschüre soll Ihnen dabei helfen, indem sie wesentliche Grundsätze unkompliziert und praxisnah darstellt.

Wir haben bewusst darauf verzichtet, die genauen gesetzlichen Vorschriften aufzuführen. Mitglieder der Geschäftsführung, Datenschutzbeauftragte, Personaler und Vorgesetzte benötigen jedoch detaillierte Kenntnisse. Denn zu ihren Aufgaben gehört es, konkrete Arbeitsanweisungen für Ihre Organisation zu erstellen und herauszugeben.

Übrigens: Auch wenn diese Broschüre von „Unternehmen“, „Geschäftsführung“ und „Beschäftigten“ spricht, gelten die Hinweise genauso auch für Vereine, Vorstände und andere Organisationen, die mit personenbezogenen Daten umgehen.

Welche Gesetze regeln das Datenschutzrecht?

Das wichtigste Gesetz für den Datenschutz ist die Europäische Datenschutzgrundverordnung[1] (DSGVO). Sie ist auch in Deutschland unmittelbar geltendes Recht. Darüber hinaus können die EU-Mitgliedsstaaten in spezifischen Bereichen eigene Regelungen erlassen. Für Deutschland wurde das Bundesdatenschutzgesetz (BDSG) entsprechend überarbeitet und angepasst. Im BDSG sind unter anderem Sonderregelungen für die Verarbeitung von Beschäftigtendaten sowie für die Zahlungseinschätzung von Schuldnern (Scoring) enthalten. Beide Gesetze sind in der Broschüre der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit dem Titel „Datenschutz-Grundverordnung“ enthalten. Sie kann dort bestellt werden. Die DSGVO ist neben vielen anderen praktischen Leitlinien auf der Seite des DatenschutzArchivs der Stiftung Datenschutz abrufbar.

https://datenschutzarchiv.org

1 Zusätzlich zu den beiden genannten Gesetzen gibt es in Deutschland eine Vielzahl von spezifischen Datenschutzvorschriften, die in verschiedenen Gesetzen verankert sind. Die Verschwiegenheitspflicht von medizinischem Personal ist beispielsweise im Strafgesetzbuch, der Umgang mit Briefen im Postgesetz und der Umgang mit Gesundheitsdaten bei Versicherungen im Sozialgesetzbuch V geregelt.

Warum Datenschutz?

Das Datenschutzrecht schützt die Rechte und Freiheiten der Menschen, wenn Organisationen personenbezogene und personenbeziehbare Daten, d. h. Informationen über einen Menschen, verarbeiten.
Es soll die Menschen vor sozial unerwünschten Folgen schützen, die durch die Verarbeitung dieser Informationen entstehen können. Dabei gilt, dass grundsätzlich jede Information über einen Menschen – beispielsweise Krankheitstage, Rentenversicherungsnummer oder Vereinsmitgliedschaft – zusammen mit anderen Informationen oder „in den falschen Händen" unerwünscht sein kann.

Damit Organisationen trotzdem Daten verarbeiten dürfen, müssen sie ihre Verarbeitungen rechtfertigen können. Die DSGVO gibt dafür die Regeln vor und ermöglicht so, dass Organisationen Daten angemessen, fair und sicher verarbeiten und die Freiheiten und Grundrechte der davon Betroffenen gewahrt bleiben. Datenschutz soll nicht die Daten an sich schützen, sondern stets die Person, auf die sich die Daten beziehen.

Dem gegenüber steht das Recht von Unternehmen, ihrem legitimen Wirtschaftsbetrieb nachzugehen und die dafür erforderlichen Daten zu verarbeiten.
Die datenschutzrechtlichen Regelungen sollen dafür sorgen, dass die Daten fair und nicht zuungunsten der betroffenen Personen verarbeiten werden. Deshalb gilt es, die notwendigen technischen und organisatorischen Vorkehrungen zu treffen, damit den Betroffenen keine unerwünschten Risiken aufgebürdet werden.

Personenbezogene Daten werden an vielen Stellen im Unternehmen verarbeitet: natürlich in der Personalabteilung (Beschäftigten- und Bewerbungsdaten), aber

auch im Einkauf (Lieferanten), im Vertrieb (Kund*innen), in der IT-Abteilung usw. Diese Daten dürfen nur für die vorher festgelegten erforderlichen betrieblichen Zwecke verwendet werden. So dürfen Vertragsdaten beispielsweise nur für Zwecke der Vertragsabwicklung verarbeitet werden. Es ist Aufgabe der Geschäftsführung, die hierfür erforderlichen Anweisungen festzulegen, aktuell zu halten und die Beschäftigten darüber zu informieren. Dazu gehört auch eine Verpflichtung der Beschäftigten, die im Dienst erlangten Informationen vertraulich zu behandeln. Damit werden sowohl Geschäftsinteressen als auch die Betroffenen geschützt.

Durch die Verarbeitung personenbezogener Daten entstehen unweigerlich Risiken für die davon betroffenen Personen. So können beispielsweise verwahrte oder gespeicherte Daten unrechtmäßig verkauft, weitergegeben sowie unbeabsichtigt verloren gehen, gelöscht werden oder in die falschen Hände geraten. Viele Unternehmen bestellen eine*n **Datenschutzbeauftragte*n**, um das Management bei der Einhaltung der gesetzlichen Vorgaben zu beraten. Ihre Aufgabe ist es auch, das Management der technischen und organisatorischen Maßnahmen, die zum Schutz vor Risiken für die betroffenen Personen erforderlich sind, zu überwachen. Wenn Sie regelmäßig 20 oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, sind Sie in Deutschland dazu verpflichtet.

Das Datenschutzrecht regelt auch, welche Maßnahmen die Datenschutzaufsichtsbehörden treffen können, wenn gegen rechtliche Vorgaben verstoßen wird. Entstehen den betroffenen Personen Nachteile oder erleiden sie Schäden, können sie Schadensersatzforderungen geltend machen. Darüber hinaus kann der Ruf des Unternehmens bei Kund*innen, Lieferanten und in der Öffentlichkeit nachhaltigen Schaden nehmen.

Was sind eigentlich personenbezogene Daten?

Personenbezogene Daten sind alle Informationen über eine natürliche Person, die sich der Person mittelbar oder unmittelbar zuordnen lassen.

- Unmittelbar zuzuordnen:
  Name, eventuell Funktion, Adresse
- Mittelbar zuzuordnen:
  Personalnummer, Kundennummer, Steuer-ID, Kontoverbindung, Cookie-ID

Übrigens: Personenbezogene Daten können auch Annahmen und Vermutungen über eine Person sein. Wenn eine Auskunftei die Kreditwürdigkeit einer Person mit Hilfe eines Score-Wertes berechnet, ist dieser Wert eine Annahme über die Zahlungsfähigkeit oder -bereitschaft des Kunden oder der Kundin bzw. über die Ausfallwahrscheinlichkeit des Kredits in der Zukunft. Auch solche Einschätzungen gehören zu den personenbezogenen Daten.

Darüber hinaus gibt es **besondere Kategorien personenbezogener Daten**, für die weitere Schutzmaßnahmen erforderlich sind. Das sind Daten, aus denen die **ethnische Herkunft**, **politische Meinungen**, **religiöse oder weltanschauliche Überzeugungen** oder eine **Gewerkschaftszugehörigkeit** hervorgehen, **genetische und biometrische Daten**, **Gesundheitsdaten** oder Daten zum **Sexualleben** oder der **geschlechtlichen Orientierung**. Für deren Verarbeitung gibt es besondere Vorschriften, für deren Einhaltung die Geschäftsführung Maßnahmen treffen und Anweisungen geben muss. Auf jeden Fall sollte bei der Verarbeitung von Daten in dieser Aufzählung immer besonders fachkundiger Rat eingeholt werden.

Wer ist für den Datenschutz im Betrieb verantwortlich?

Noch einmal zur Erinnerung: Alles, was hier zu „Unternehmen“ und „Mitarbeitenden“ gesagt wird, betrifft in gleicher Weise auch andere Organisationen, wie Vereine, Stiftungen, öffentliche und kommunale Einrichtungen sowie deren Beschäftigte, Ehrenamtliche, Praktikantinnen usw.

DIE UNTERNEHMENSLEITUNG SCHAFFT DIE RAHMENBEDINGUNGEN

Mitarbeitende dürfen personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten. Daher ist die Unternehmensleitung verpflichtet, genaue Anweisungen für den Datenumgang herauszugeben. Ohne eine solche Weisung dürfen Daten nur dann verarbeitet werden, wenn es eine gesetzliche Verpflichtung dafür gibt. Darüber hinaus sollten Vorgesetzte jederzeit in der Lage sein, datenschutzrelevante Anweisungen zu erteilen und Fragen zu beantworten.

BESCHÄFTIGTE WENDEN DIE ANWEISUNGEN AN

Beispiele

- Sie erfassen eingehende Bewerbungen. Dürfen Sie dazu Daten aus den sozialen Netzwerken ergänzen?
- Sie erstellen ein Rundschreiben an alle Kunden und schicken deren Adressen an die Druckerei. Ist diese Datenweitergabe vertraglich geregelt? Ist sie zulässig und erfolgt sie in gesicherter Form?
- Ein wichtiger Kunde erzählt am Telefon, dass er heute Geburtstag hat. Dürfen Sie diese Information in der Kundendatenbank speichern?

Wenn Sie personenbezogene Daten verarbeiten, prüfen Sie Ihr Vorgehen in zwei Schritten:

1. Gibt es eine Arbeitsanweisung, die vorgibt, wie die konkrete Aufgabe rechtskonform und datensicher zu erledigen ist? Dann folgen Sie dieser Anweisung.
2. Gibt es keine Anweisung zur Datenverarbeitung, entscheiden Sie selbst über die datenschutzrechtlich korrekte Verarbeitung. Falls Sie bei der Bewertung unsicher sind, müssen Sie sich an Ihren Vorgesetzten oder den betrieblichen Datenschutzbeauftragten wenden.

„Daumenregel“

Manchmal liegt es auf der Hand, manchmal ist es unklar, ob die eine Datenverarbeitung datenschutzrechtlich zulässig ist. Hier könnte Ihnen dieser zweistufige „Test“ helfen:

Dient die Datenverarbeitung einem legitimen Zweck, z. B. der Vertragsabwicklung mit einem Kunden oder Beschäftigten? Wenn ja, könnte der Vertrag auch dann erfüllt werden, wenn die Daten oder ein einzelnes Datum wegfällt? Ist dies der Fall, ist eine Datenverarbeitung nicht erforderlich und darf darum nicht erfolgen. Sie sollten sich in diesem Fall oder im Zweifel an Ihren Vorgesetzten oder Ihren Datenschutzbeauftragten wenden.

BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Betriebliche Datenschutzbeauftragte beraten in Unternehmen über die Möglichkeiten, wie personenbezogene Daten rechtskonform verarbeitet werden können und überprüfen das Management der datenschutzrechtlichen Maßnahmen. Unternehmen in Deutschland müssen eine*n betrieblichen Datenschutzbeauftragte*n stellen, wenn sie in der Regel 20 Personen oder mehr ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Aufgabe der Datenschutzbeauftragten ist es, Geschäftsleitung und Beschäftigte hinsichtlich datenschutzkonformer Datenverarbeitung zu beraten. Die Aufgabe, den Datenschutz sicherzustellen, haben sie dagegen nicht. Diese Aufgabe liegt bei der Unternehmensleitung. Als unabhängiger und zur Verschwiegenheit verpflichteter Berater und Kontrolleur steht der Datenschutzbeauftragte aber als Ansprechpartner für alle Beschäftigten zur Verfügung. Jede Meldung zu datenschutzrelevanten Umständen im Unternehmen wird er vertraulich behandeln. Sollten Sie Fragen zum Datenschutz haben, können Sie sich also nicht nur an Ihre Vorgesetzten wenden, sondern jederzeit auch den betrieblichen Datenschutzbeauftragten ansprechen, ohne befürchten zu müssen, dass sich das für Sie nachteilig auswirkt.

DIE DATENSCHUTZAUFSICHTSBEHÖRDE BERÄT, KONTROLLIERT UND VERHÄNGT EVENTUELL BUSSGELDER

Für jedes Unternehmen gibt es eine zuständige Behörde, die den Datenschutz überwachen soll und Anzeigen und Beschwerden von Betroffenen bearbeitet. Für die meisten Unternehmen in Deutschland ist diese Behörde der oder die **Landesbeauftragte** für den Datenschutz und in Bayern das Landesamt für Datenschutzaufsicht. Der oder die **Bundesbeauftragte** für den Datenschutz ist für Bundesbehörden und für die Unternehmen der Telekommunikations- und Postbranche zuständig.

Die Datenschutzbehörden können Unternehmen aufgrund einer Beschwerde oder auch anlasslos prüfen. Stellt die Behörde unzureichende Maßnahmen oder einen Verstoß gegen das Datenschutzrecht fest, kann sie Hinweise geben und das Unternehmen zur Nachbesserung auffordern, die Verarbeitung untersagen sowie Bußgelder bis zu 20 Mio. Euro oder von bis zu vier Prozent des weltweiten Jahresumsatzes verhängen.

Vier Pflichten für den Datenschutz

Die Datenschutzgesetze sehen für den Datenumgang die folgenden vier Pflichten vor:

1. Die Datenverarbeitung muss durch eine Rechtsgrundlage überhaupt erlaubt sein.
2. Die Betroffenen müssen über die Verarbeitung ihrer Daten informiert sein.
3. Die Datenverarbeitung muss durch Maßnahmen sicher gestaltet sein.
4. Die Daten müssen gelöscht werden, sobald sie für den Zweck der Verarbeitung nicht mehr erforderlich sind.

IST DIE DATENVERARBEITUNG ERLAUBT?

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn eine der folgenden Anforderungen gegeben ist:

- es liegt eine Einwilligung der Person vor, deren Daten verarbeitet werden sollen
- es gibt einen Vertrag, eine Betriebsvereinbarung, oder auf Wunsch des Kunden soll ein Vertrag vorbereitet werden
- es liegt eine Notsituation für Leib oder Leben vor, die die Verarbeitung erforderlich macht
- es gibt eine Rechtsvorschrift, die die Datenverarbeitung erforderlich macht
- das Interesse des Unternehmens an der Datenverarbeitung überwiegt gegenüber dem Interesse der Person daran, dass die Daten nicht verarbeitet werden.

Entscheidend ist dabei immer, ob die personen-

bezogenen Daten auch tatsächlich erforderlich sind, um den konkreten Zweck zu erreichen. Um dies zu entscheiden, hilft der zweistufige Test.

Beispiele für erlaubte Datenverarbeitung

- Die E-Mail-Adresse darf gespeichert werden, wenn und solange ein*e Kund*in einen Newsletter bestellt hat.
- Die Personalabteilung darf Lebensläufe und Zeugnisse der Beschäftigten für Zwecke der Einstellung und der Personalverwaltung speichern.
- Die Personalabteilung darf Lebensläufe und Zeugnisse von abgelehnten Bewerbenden nur dann in einem Bewerberpool für spätere Stellenbesetzungen speichern, wenn die Bewerbenden dem zuvor ausdrücklich zugestimmt haben.
- Die Betriebsrevision darf Beschäftigtendaten erheben, um die korrekten Abläufe des Unternehmens zu prüfen. Dabei ist es datenschutzrechtlich geboten, die Daten nicht unter dem konkreten Namen, sondern unter einem Code zu erheben (pseudonymisierte Daten).
- Die IT-Abteilung ist zur Bereitstellung des Netzwerkverkehrs oder zur SPAM-Kontrolle befugt, eine Vielzahl von Inhalten des Netzverkehrs automatisiert zu prüfen und zu filtern.

Ihre Prüffrage

Gibt es eine Vorschrift, eine Betriebsvereinbarung, einen Vertrag, ein objektiv überwiegendes Interesse oder eine Einwilligung, die zulässt, dass die Informationen über die betroffenen Personen aufbereitet, weitergegeben oder sonst genutzt werden?

IST DIE BETROFFENE PERSON ÜBER DIE DATENVERARBEITUNG INFORMIERT?

Die betroffene Person muss klar erkennen können, dass personenbezogene Daten über sie gespeichert und verarbeitet werden: von welchem Unternehmen und zu welchem Zweck dies geschieht, um welche Daten es sich handelt und ggfs. ob diese Daten weitergegeben werden. Auch ein Hinweis auf ein Widerspruchsrecht ist ein Muss.

Ihre Checkliste zur Informationspflicht

Ist die betroffene Person hinreichend informiert über

- ☐ den vollständigen Namen und
- ☐ die vollständige Adresse Ihres Unternehmens,
- ☐ eine Adresse für Datenschutzfragen (z. B. datenschutz@unternehmen.de),
- ☐ alle Zwecke, für die die Daten der betroffenen Person verwendet werden, einschließlich der Rechtsgrundlage der Verarbeitung und der „berechtigten Interessen", falls die Erlaubnis aus einer Interessenabwägung resultiert,
- ☐ die Kategorien von Empfängern der Daten, falls die Datenweitergabe geplant ist,
- ☐ eine eventuelle Verarbeitung der Daten außerhalb des europäischen Wirtschaftsraums,
- ☐ den Zeitpunkt, zu dem die Daten gelöscht werden, bzw. zu dem der Zugriff auf die Daten eingeschränkt wird,
- ☐ ihre Betroffenenrechte, also ihre Widerrufsrechte, ihre Beschwerderechte oder die Tatsache, dass eine Entscheidung – zum Beispiel über eine Kreditvergabe – nach automatischen Berechnungen direkt von einem IT-System getroffen wird?

ERFOLGT DIE VERARBEITUNG DER DATEN SICHER?

Unternehmen wie Beschäftigte müssen technische Vorkehrungen treffen, damit die Verarbeitung personenbezogener Daten sicher erfolgt. Dafür ist vorab zu bestimmen, wer für die Verarbeitung der personenbezogenen Daten für die festgelegten Zwecke zuständig sein soll. Personenbezogene Daten müssen so verarbeitet werden, dass sie nicht abhandenkommen und nicht von Unbefugten – auch innerhalb des Unternehmens – eingesehen oder verändert werden können. Wenn personenbezogene Daten weitergegeben werden müssen, dann nur mit entsprechenden Sicherheitsmaßnahmen. Es ist daher arbeitsvertragliche Nebenpflicht, sowohl die Informationen über natürliche Personen als auch vertrauliche Firmeninformationen vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen.

DATENSICHERHEITSREGELN

Datenerfassung
Erfasst werden dürfen nur die für vorher festgelegte Zwecke erforderlichen Informationen. Ein Zuviel an personenbezogenen Daten ist rechtswidrig. Das ist auch deshalb wichtig, weil die betroffenen Personen Auskunft über ihre im Unternehmen gespeicherten Daten verlangen können. Das Unternehmen ist dann verpflichtet, alle über die betroffene Person gespeicherten Daten offen zu legen.

Papierakten
Dokumente mit personenbezogenen Daten dürfen nicht in den normalen Müll oder Altpapiercontainer, sondern müssen entweder mit einem Aktenvernichter vernichtet oder in dafür vorgesehenen Datenabfallbehältern entsorgt werden.

Kommunikation
Seien Sie grundsätzlich bei der Weitergabe von Daten vorsichtig. Achten Sie stets sorgfältig darauf, die richtige E-Mail-Adresse und Faxnummer einzugeben. Und überprüfen Sie auch, ob die Person hinter der E-Mail-Adresse oder Faxnummer berechtigt ist, die Informationen zu empfangen. Vertrauen Sie nie einfach auf eine am Telefon mitgeteilte Faxnummer oder E-Mail-Adresse. Verlangt beispielsweise eine Person telefonisch Informationen zu einem Vertrag und gibt dann eine Faxnummer oder E-Mail-Adresse an, kann es sich auch um einen Trick handeln.

Greifen Sie im Zweifel immer auf den Postversand an eine bestätigte Adresse zurück. Stellen Sie bei der Übermittlung von wichtigen personenbezogenen Daten (vor allem Personaldaten, Gesundheitsdaten) eine persönliche Entgegennahme sicher und verschlüsseln Sie das Dokument, wenn Sie es als Anhang zu einer E-Mail versenden. Versenden Sie geheimhaltungs-

bedürftige und personenbezogene Daten daher in der Regel verschlüsselt oder per Post.

Datentransport
Außerhalb der Betriebsräume sind personenbezogene Daten stets auf firmeneigenen portablen Datenträgern (USB-Sticks, Festplatten) und nur verschlüsselt zu transportieren. Fremde Datenträger dürfen nicht ungeprüft verwendet werden.

Datenverlust
Wenn Daten verloren werden (USB-Stick liegengelassen, E-Mail mit Anhang an falschen Adressaten gesendet), ist der für Ihr Unternehmen geltende Meldeweg zu beachten, also z. B. der Vorgesetzte, der betriebliche Datenschutzbeauftragte, die Geschäftsleitung (siehe Abschnitt „Verhalten bei Datenlecks“).

Verschlüsselung, Passwörter
Meist geben Unternehmen entsprechende Arbeitsanweisungen heraus, wie Daten zu verschlüsseln und Passwörter zu organisieren sind. Informationen dazu finden Sie auch beim Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de), dessen Empfehlungen auch für den privaten Bereich sinnvoll sind.

Beim Verlassen des Rechners ist dieser zu sperren (bei Windows-Rechnern: WINDOWS-Taste + L, bei Mac-Rechnern: Control + Command + Q). Eine Reaktivierung darf nur über eine Passworteingabe möglich sein. Zusätzlich muss die Sperrung nach vorgegebener Zeit automatisch aktiviert werden, damit kein Unbefugter den Computer benutzen kann, wenn Sie das Sperren einmal versäumt haben.

Vertrauliche Gespräche
Führen Sie Gespräche und Telefonate mit vertraulichen Inhalten so, dass Unbefugte das Gespräch nicht mithören können.

Allgemeine Wachsamkeit
Sprechen Sie Personen an, die Sie nicht kennen und die Ihnen auf dem Firmengelände auffallen, und fragen Sie sie gegebenenfalls nach Namen und Funktion. Melden Sie Ihre Beobachtungen; gehen Sie nicht achtlos vorbei.

Wenn Ihnen etwas auffällt
Wenn Sie bemerken oder vermuten, dass es im Unternehmen einen Datenschutzverstoß gibt, wenden Sie sich an Ihre Vorgesetzten oder die Datenschutzbeauftragte. Datenschutzbeauftragte müssen Ihre Angaben vertraulich behandeln und sind auch gegenüber der Unternehmensleitung zur Verschwiegenheit verpflichtet.

Ihre Prüffrage

Habe ich alles in meiner Macht Stehende getan, so dass meine für die konkrete Sache nicht zuständigen Kolleg*innen und außenstehende Dritte vom Inhalt meiner Datenverarbeitung keine Kenntnis erhalten? Habe ich alle Vorgaben befolgt?

DATEN AUFBEWAHREN, LÖSCHEN ODER DEN ZUGRIFF EINSCHRÄNKEN?

Jedes Unternehmen muss sicherstellen, dass nach Ablauf der Erforderlichkeit der Datenspeicherung oder der gesetzlichen Fristen der Zugriff auf personenbezogene Daten eingeschränkt wird bzw. die betreffenden Daten gelöscht werden.

Beispiel

Es ist zulässig, bestimmte Bereiche des Betriebs, wie z. B. den Eingang zum Lager, per Videokamera zu überwachen. Grundsätzlich muss dafür ein begründetes Sicherheitsinteresse bestehen. Doch auf die Aufzeichnungen der Videokameras darf nur ein ganz eingeschränkter Personenkreis zugreifen, der Zugriff muss protokolliert werden und nach Ablauf von wenigen Tagen müssen die Aufnahmen durch Überschreiben gelöscht werden. Videobilder dürfen aber z. B. nicht dafür genutzt werden, über Wochen hinweg das Kommen und Gehen einzelner Mitarbeitender zu ermitteln. Tabu sind auch Aufenthalts- und Sozialräume.

Personenbezogene Daten, die vom Unternehmen verarbeitet werden, dürfen nicht durch Beschäftigte nach Gutdünken gelöscht werden. Für das Löschen muss die Unternehmensleitung Arbeitsanweisungen herausgeben.

Beispiel

Bewerbungsunterlagen müssen drei Monate nach der Besetzung der Stelle gelöscht werden, d. h. die Unterlagen sind an die abgelehnten Bewerber zurückzuschicken oder zu vernichten. Reisekostenabrechnungen für Bewerbungsgespräche mit der Adresse der Bewerbenden müssen jedoch für die Buchhaltung zehn Jahre lang aufbewahrt werden.

Die Pflicht zu löschen gilt für alle Speicherorte (E-Mail-Accounts, Webserver, Cloud-Speicher) und natürlich auch für gedruckte Fassungen von elektronischen Daten.

Den Löschpflichten gegenüber stehen die gesetzlichen Aufbewahrungsfristen, zum Beispiel für das Finanzamt. Während also Zeugnisse der Bewerbenden nach drei

Verhalten bei Datenlecks

Kein Unternehmen ist zu 100 Prozent sicher. Damit Datenschutzvorfälle nicht verheimlicht werden, müssen sie der zuständigen Datenschutzaufsichtsbehörde gemeldet werden. Das ist Aufgabe der Geschäftsführung bzw. des Datenschutzbeauftragten.
Sie persönlich sollten jederzeit nachweisen können, dass Sie Ihre Meldepflicht erfüllt haben.

Ihre Vorgehensweise bei einer Datenschutzverletzung

Wenn Sie einen Datenschutzvorfall erkennen, wenden Sie sich sofort an Ihren Vorgesetzten und an den oder die betriebliche Datenschutzbeauftragte. Erstellen Sie einen kurzen Bericht: Welche Daten sind abgeflossen oder waren im Zugriff? Wie ist es dazu gekommen? Welche Folgen vermuten Sie? Senden Sie diesen Bericht an Ihre Vorgesetzte und den betrieblichen Datenschutzbeauftragten.

Herausgeber
Stiftung Datenschutz

Autor*innen
Autor der Erstausgabe: Dr. Philipp Kramer
Überarbeitung der Erstausgabe: Kirsten Bock

Über die Autor*innen

Dr. Philipp Kramer ist Rechtsanwalt in Hamburg. Er berät internationale Konzerne und mittelständische Unternehmen in den Fachgebieten Datenschutzrecht, Neue Medien, IT-Recht, Urheberrecht. Er veröffentlicht regelmäßig zu Themen des IT–Rechts und hält Vorträge auf Seminaren zu den Themen des Datenschutzes, der IT-Sicherheit und des Wettbewerbsrechts. Zudem ist er Chefredakteur des Datenschutz-Berater und erster Vorsitzender der Hamburger Datenschutzgesellschaft HDG e.V. sowie Lehrbeauftragter der Universität Hamburg und Lehrbeauftragter der Hochschule Ulm.

Kirsten Bock ist Interimsvorständin und Wissenschaftliche Leiterin der Stiftung Datenschutz mit umfangreichem und vielfältigem Erfahrungsschatz. Sie bearbeitet Problemstellungen zum Datenschutzrecht, zur Anonymisierung von Daten sowie zur Zertifizierung von Datenschutzbeauftragten und betreut wissenschaftliche Projekte. Sie hat an der Entwicklung des Standard-Datenschutzmodells (SDM) mitgewirkt und als Leiterin des Europäischen Datenschutzgütesiegels EuroPriSe am Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein ein komplexes Prüf- und Beratungsverfahren im internationalen Datenschutzbereich aufgebaut. In zahlreichen Gremien und Arbeitsgruppen auf internationaler, europäischer und auf Bundesebene hat sie an der Gestaltung des Datenschutzrechts und internationaler Vereinbarungen mitgewirkt. Darüber hinaus war sie Mitglied des Wissenschafts- und Innovationsbeirats Registermodernisierung des Bundes.

Über die Stiftung Datenschutz

Die Stiftung Datenschutz wurde 2013 von der Bundesregierung gegründet. Stifterin ist die Bundesrepublik Deutschland. Aufgabe der unabhängigen Einrichtung ist die Förderung des Datenschutzes an den Schnittstellen zwischen Politik, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Gesellschaft.

Die Bundesstiftung bietet eine neutrale Diskussionsplattform zu Fragen der Datenpolitik und des Datenschutzrechts. Darüber hinaus stellt sie praktische Informationen zur Anwendung des Datenschutzrechts für verschiedene Zielgruppen bereit.

Die Stiftung Datenschutz ist gemeinnützig und neutral; sie agiert frei von gewerblichen oder aufsichtspolitischen Interessen.

STIFTUNG DATENSCHUTZ

Bundesministerium der Justiz und für Verbraucherschutz

Stiftung Datenschutz
Kirsten Bock (V.i.S.d.P.)

Karl-Rothe-Straße 10–14
04105 Leipzig
T 0341 5861 555-0
F 0341 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJV).

Ihre Notizen

Version 2.2, Stand September 2026

Die Erstausgabe der Broschüre ist eine gekürzte Fassung von „Datenschutz im Betrieb“ verfasst von Rechtsanwalt Dr. Philipp Kramer im Auftrag der Stiftung Datenschutz.

Das Werk ist folgendermaßen lizenziert unter Creative Commons: „Namensnennung – Nicht kommerziell – Keine Bearbeitungen“ (genaue Bedingungen unter: http://creativecommons.org/licenses/by-nc-nd/4.0).