DATENSCHUTZ IM BETRIEB

Eine Handreichung für Beschäftigte

STIFTUNG DATENSCHUTZ

LIEBE LESERINNEN UND LESER,

ganz gleich, welche Größe der Betrieb hat, bei dem Sie beschäftigt sind – Ihr Arbeitgeber muss sicherstellen, dass die Regeln zum Datenschutz eingehalten werden. Doch kann ein Unternehmen nur dann gesetzeskonform handeln, wenn auch seine Mitarbeiterinnen und Mitarbeiter die Vorgaben kennen und bei ihrer täglichen Arbeit befolgen. Dabei soll Ihnen diese Broschüre helfen. Damit möchte die Stiftung Datenschutz einen konkreten Beitrag zur Aufklärung über die Regeln zum Datenschutz für alle Beschäftigten leisten – besonders im Mittelstand, für den die seit Mai 2018 anzuwendende EU-Datenschutzgrundverordnung oft eine besondere Herausforderung darstellt.

Wir arbeiten im Text dieses Heftes mit lebensnahen Praxisbeispielen und möchten Ihnen den Datenschutz näherbringen – als eine Aufgabe, die gemeistert werden kann. Dafür ist an vielen Stellen eine grundlegende Sensibilität bereits hilfreich: Sie müssen nicht immer die exakten Rechtsvorschriften kennen, aber ein gewisses Gefühl ist wichtig, ob ein Umgang mit Informationen gegen das Gesetz verstoßen könnte. Wenn Sie in einer solchen Situation bei Ihren Vorgesetzten, beim betrieblichen Datenschutzbeauftragten oder bei der Rechtsabteilung nachfragen, dann tragen Sie zum datenschutzgerechten Handeln in Ihrem Unternehmen bei.

Unsere Hinweise richten sich an Geschäftsführungen, Beschäftigte in Personal- und IT-Abteilungen, Freiberufler, Gewerbetreibende und auch sonst an alle, die in ihrer täglichen Arbeit mit personenbezogenen Daten umgehen müssen. Die meisten von Ihnen sind sicher juristische Laien. Um die Lesbarkeit der Broschüre zu steigern, haben wir deshalb nicht immer die üblichen juristischen Fachbegriffe verwendet, sondern versucht, eine für alle verständliche Sprache zu nutzen.

Auch wenn wir durchgehend von „Unternehmen“, „Geschäftsführern“ und „Beschäftigten“ sprechen, gelten die Hinweise genauso auch für Vereine, Vorstände und andere Organisationen und Personen.

Wenn Sie Anregungen, Kritik oder Verbesserungsvorschläge zu „Datenschutz im Betrieb“ haben, melden Sie sich gerne bei uns: mail@stiftungdatenschutz.org

Freundliche Grüße von

Frederick Richter
Vorstand der Stiftung Datenschutz

INHALT

FÜR WEN IST DIESE BROSCHÜRE GEDACHT?

FÜR DIE BESCHÄFTIGTEN

Jeder Beschäftigte, der aktiv für das Unternehmen tätig ist, ob als Manager oder als Praktikant, muss sich mit den Kernpflichten des Datenschutzes auskennen. Zwar müssen sich vertieft mit den gesetzlichen Vorschriften zum Datenschutz nur die Unternehmensleitung, die Rechtsabteilung und der oder die betriebliche Datenschutzbeauftragte befassen, doch trifft in der heutigen Arbeitswelt nahezu jeder Beschäftigte auch eigene Entscheidungen zur Datenverarbeitung.

Auch wenn Sie nicht ständig – wie zum Beispiel in der Personal-, der Marketing- oder der IT-Abteilung – mit personenbezogenen Daten arbeiten, müssen Sie die rechtlichen Vorgaben beachten und anwenden, wenn Sie Sanktionen und nachteilige Folgen für Ihr Unternehmen oder sogar für Sie selbst vermeiden wollen. Dabei will diese Broschüre helfen. Sie ergänzt damit die Arbeitsanweisungen, die Ihre Geschäftsleitung zum Datenumgang möglicherweise erlassen hat.

FÜR DIE UNTERNEHMENSLEITUNG

Als Unternehmensleitung sind Sie verpflichtet, Ihre Belegschaft zum Datenschutz aufzuklären. Das bedeutet, dass Ihre Mitarbeiterinnen und Mitarbeiter wissen, dass sie personenbezogene Daten nur nach Ihrer Weisung verarbeiten dürfen. Sie können diese Handreichung einsetzen, um die Beschäftigten zu sensibilisieren und über die grundlegenden Anforderungen aufzuklären.

Diese Broschüre kann konkrete Arbeitsanweisungen zum Umgang mit bestimmten Datenarten nicht ersetzen und ist daher ggf. durch weitere Anweisungen zu ergänzen. Die Broschüre liefert jedoch die gesetzlich vorgesehenen Grundinformationen und allgemeine datenschutzbezogene Arbeitsanweisungen.

FÜR DIE BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Als betrieblicher Datenschutzbeauftragter gehört es zu Ihren Aufgaben, „die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der Datenschutz-Grundverordnung sowie nach sonstigen Datenschutzvorschriften“ zu unterrichten und zu beraten (Art. 39 DSGVO). Hierzu können Sie Präsenz- oder Online-Schulungen anbieten, aber auch diese Handreichung einsetzen.

DATENSCHUTZ IM UNTERNEHMEN

GEHEIMNISSE IM UNTERNEHMEN

Betriebs- und Geschäftsgeheimnisse

Unternehmen und andere Organisationen verfügen über **Informationen**, die **nur bestimmten Personengruppen bekannt** sind und die nicht an die Öffentlichkeit gelangen sollen. Diese werden üblicherweise als Betriebs- oder Geschäftsgeheimnisse bezeichnet. Typische Geschäftsgeheimnisse sind Rezepturen, Produktionsverfahren und Informationen über finanzielle Verhältnisse.

Beschäftigte, denen Betriebs- oder Geschäftsgeheimnisse im Rahmen ihrer Tätigkeit bekannt sind, müssen diese geheim halten; so sehen es die deutschen Gesetze vor. Die Unternehmensleitung sorgt üblicherweise dafür, dass diese **Geheimhaltung vertraglich vereinbart** wird – nicht nur mit Mitarbeitern in Arbeitsverträgen, sondern auch mit externen Dienstleistern wie Zeitarbeitsfirmen oder Lieferanten in den Dienstleistungsverträgen. So verpflichten sich die Vertragspartner, Betriebs- und Geschäftsgeheimnisse zu wahren.

Vertraulichkeit und Datenschutz

Auch Informationen über natürliche Personen gehören zu den Betriebs- und Geschäftsgeheimnissen, zum Beispiel die in der Personalabteilung vorliegenden Informationen über Mitarbeiter.

Diese „personenbezogenen Daten“ sind besonders geschützt: durch die europäische **Datenschutz-Grundverordnung** und in Deutschland durch das ergän-

zende Bundesdatenschutzgesetz. Das Ziel des Datenschutzes besteht darin zu verhindern, dass **Unbefugte** an **Informationen über eine natürliche Person** gelangen können oder dass Inhaber von solchen Informationen diese in ungerechtfertigter Weise nutzen.

Die Vorschriften sind streng. Ein Datenschutzverstoß kann bereits vorliegen, wenn

- personenbezogene Daten gespeichert oder kopiert werden, die für die Arbeitsaufgaben nicht benötigt werden,
- Informationen über Kunden weitergeleitet werden, ohne dass es dafür eine Erlaubnis gibt,
- personenbezogene Daten ohne Zustimmung der betroffenen Person unverschlüsselt per E-Mail verschickt werden.

Was genau sind „personenbezogene Daten“?

Personenbezogene Daten sind alle **Informationen über eine natürliche Person**, die sich der Person mittelbar oder unmittelbar zuordnen lassen. Das betrifft Mitglieder der Geschäftsleitung ebenso wie Mitarbeiterinnen und Mitarbeiter, Beschäftigte von Lieferanten ebenso wie Gäste und Kunden oder Interessenten.

Beispiele

- Unmittelbar zuzuordnen ist der Person ihr Name.
- Unmittelbar zuzuordnen ist der Person auch ihre Funktion, wenn es zum Beispiel nur eine IT-Leiterin im Unternehmen gibt.
- Mittelbar zuzuordnen ist der Person ihre Personalnummer: Zwar weist die Personalnummer an sich noch nicht auf die konkrete Person hin, der

Personenbezug kann jedoch von Personen hergestellt werden, die wissen, welcher Name zu welcher Personalnummer gehört.

- Mittelbar kann sogar eine IP-Adresse einer bestimmten Person zugeordnet werden.

Diese Beispiele zeigen, dass vor allem beim **mittelbaren Personenbezug** der Zusammenhang betrachtet werden muss, wenn es darum geht zu entscheiden, ob es sich um personenbezogene Daten handelt.

Übrigens: Personenbezogene Daten können auch **Annahmen und Vermutungen** 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 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**, die noch strenger geschützt 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; deshalb soll der Umgang mit diesen Daten hier nicht weiter betrachtet werden. Auf jeden Fall sollte bei der Verarbeitung von Daten in dieser Aufzählung immer besonders fachkundiger Rat eingeholt werden.

BETRIEBSGEHEIMNISSE UND DATENSCHUTZ

Neben Geschäfts- und Betriebsgeheimnissen unterliegen auch personenbezogene Daten einem besonderen Schutz. Bei ihrer Verarbeitung müssen umfangreiche Datenschutzvorschriften beachtet werden, denn Verstöße – nicht nur vorsätzliche, sondern auch fahrlässige (also aus Unwissenheit oder Nachlässigkeit) – können zu nachteiligen Folgen für das Unternehmen und auch für den handelnden Mitarbeiter führen. In erster Linie geht es natürlich darum, Nachteile von den Betroffenen aus rechtswidriger oder datenunsicherer Verarbeitung fernzuhalten. Die vorliegende Broschüre gibt Ihnen einen grundlegenden Überblick über die gesetzlichen Vorschriften und zahlreiche Tipps für die Praxis. Sie soll Ihnen helfen, im Arbeitsalltag die richtigen Entscheidungen für den Datenschutz zu treffen.

DIE BEDEUTUNG DES DATENSCHUTZES IM UNTERNEHMEN

Durch die Datenschutzvorschriften werden personenbezogene Daten im Unternehmen nicht nur als Wirtschaftsgut des Unternehmens geschützt. Vor allem die Personen, deren Daten verarbeitet werden, sollen geschützt sein. Damit will der Gesetzgeber verhindern, dass Menschen durch unbefugten oder unsachgemäßen Umgang mit ihren Daten Schaden erleiden.

Beispiele für unsachgemäßen Umgang mit personenbezogenen Daten

Ein Angestellter der Personalabteilung will einen Vorgesetzten über ein ärztliches Beschäftigungsverbot einer Mitarbeiterin per unverschlüsselter E-Mail informieren. Bei der Adresseingabe vertippt er sich und schickt die Mail mit den sensiblen gesundheitsbezogenen Daten versehentlich an die Kollegen der Betroffenen.

Als Service für die Kunden veröffentlicht ein Unternehmen die Mobilfunknummern wichtiger Ansprechpartner auf seiner Website. Nach Feierabend erhält der Produktionsleiter nun regelmäßig Anrufe von Unternehmen, die ihre Produkte verkaufen oder ihn abwerben wollen.

Hinter dem Datenschutzrecht steht das Konzept, dass jeder Mensch grundsätzlich selbst entscheiden können soll, welche seiner persönlichen Daten wem wann zugänglich sein sollen (das sogenannte „Recht auf informationelle Selbstbestimmung“). Wichtig zum Verständnis: **Datenschutz soll nicht die Daten an sich schützen. Es geht immer um den Menschen, auf den sich die Daten beziehen.** Datenschutz ist Persönlichkeitsschutz – und kein Selbstzweck! Dem Anliegen eines starken Persönlichkeitsschutzes gegenüber steht das Recht des Unternehmens, wirtschaftlich mit Daten zu arbeiten. Das Datenschutzrecht regelt, in welcher Situation welches der beiden Rechte überwiegen soll.

Stets müssen Unternehmen und Organisationen für den gesetzeskonformen Umgang mit personenbezogenen Daten sorgen. Dazu ergreifen sie üblicherweise bestimmte **Maßnahmen**:

Beispielsweise müssen Beschäftigte, die mit personenbezogenen Daten arbeiten (in der Personalabteilung, in der IT, im Kundenservice, im Vertrieb, im Betriebsrat…) über **datenschutzgerechtes Verhalten belehrt** werden.

Viele Unternehmen bestellen auch einen **Datenschutzbeauftragten** Dazu sind sie in Deutschland verpflichtet, wenn sie regelmäßig 20 oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Dessen Kontaktdaten müssen dann auch der

Aufsichtsbehörde mitgeteilt werden. Mehr zur Rolle des Datenschutzbeauftragten finden Sie im Abschnitt „Wer sorgt für guten Datenschutz?“

Die Unternehmensleitung muss über **Arbeitsanweisungen** den Umgang mit personenbezogenen Daten regeln. Allerdings gibt es Arbeitsabläufe, die das Unternehmen nicht bis ins kleinste Detail vorgeben kann. Dann müssen Mitarbeiter selbst die relevanten Datenschutzvorschriften anwenden und entscheiden, ob eine bestimmte Verarbeitung der Daten zulässig ist oder nicht. Betroffen sind nicht nur Abteilungen, in denen intensiv mit personenbezogenen Daten umgegangen wird, wie Personalabteilungen; auch sonst treffen viele Beschäftigte im Arbeitsalltag für das Unternehmen eigene Datenverarbeitungsentscheidungen, sei es beim **Versand einer E-Mail** oder bei der **Eingabe von Personendaten in Unternehmensdatenbanken**. Dabei sind stets gesetzliche Datenschutzpflichten zu berücksichtigen, andernfalls drohen dem Unternehmen – und u.U. sogar den handelnden Beschäftigten – Sanktionen und andere nachteilige Folgen. Mehr dazu finden Sie im Abschnitt „Haftung bei Datenschutzverstößen“.

Unternehmen selbst haben ein großes Interesse daran, dass alle ihre Prozesse datenschutzkonform sind, um Gesetzesverstöße mit Haftungsgefahren und Risiken für ihre Reputation zu vermeiden. Auch die Öffentlichkeit ist in den vergangenen Jahren in Bezug auf den sorgfältigen Umgang mit personenbezogenen Daten sensibler geworden; Datenpannen beschädigen den Ruf des Unternehmens bei Kunden und Lieferanten und können – neben der Verletzung der Rechte der Betroffenen – auch nachhaltigen wirtschaftlichen Schaden verursachen.

FAZIT

DATENSCHUTZZWECKE

Das Datenschutzrecht will Menschen davor schützen, dass ihre Daten unbefugt verwendet werden oder ihnen durch den Umgang mit sie betreffenden Daten Schaden entsteht.

RECHTLICHE GRUNDLAGEN

WELCHE GESETZE REGELN DEN DATENSCHUTZ?

Das wichtigste Gesetz für den Datenschutz ist die Europäische **Datenschutz-Grundverordnung**[1] (DSGVO), die seit Mai 2018 in allen EU-Mitgliedsstaaten gilt. Ergänzend können sich die EU-Mitgliedsstaaten eigene Regelungen geben. Für Deutschland ist dies das Bundesdatenschutzgesetz, das überarbeitet und angepaßt wurde. In diesem Begleitgesetz finden sich u.a. **Sonderregelungen** für die Verarbeitung von Beschäftigtendaten und für die Zahlungseinschätzung von Schuldnern (Scoring).

Beide Gesetze sind in der Broschüre des Bundesbeauftragten für den Datenschutz „Datenschutz-Grundverordnung“ enthalten. Sie ist neben vielen weiteren Materialien abrufbar auf der Informationsplattform der Stiftung Datenschutz zur Umsetzung der EU-Datenschutzreform[2].

Darüber hinaus gibt es in Deutschland eine Vielzahl von speziellen Datenschutzvorschriften in ganz unterschiedlichen Gesetzen. So ist beispielsweise die Verschwiegenheitspflicht von medizinischem Personal im Strafgesetzbuch, der Umgang mit Briefen im Postgesetz und der Umgang mit Gesundheitsdaten bei Versicherungen im Sozialgesetzbuch V geregelt.

Das Datenschutzrecht **schützt personenbezogene Daten in jeder Form, nicht nur auf Computern oder in Datenbanken, sondern auch in Papier-Karteien**. Nur ungeordnete Informationen auf losen Zetteln oder lediglich mündlich ausgetauschte personenbezogene Daten fallen nicht unter das Datenschutzrecht. Eine Ausnahme von dieser Ausnahme betrifft Beschäftigtendaten; bei denen ist das Gesetz in Deutschland besonders streng und erfasst bereits den mündlichen Austausch zwischen zwei Personen. Schickt also ein Mitarbeiter der Personalabteilung einer Kollegin aus dem Vertrieb nicht allgemein bekannte Informationen über einen Kollegen, so ist das ohne arbeitsrechtlichen Sachgrund oder ohne Einwilligung des betroffenen Kollegen rechtswidrig.

1 http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

2 DSGVO.stiftungdatenschutz.org

WANN LÄSST DAS DATENSCHUTZRECHT DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN ZU?

Auch unter der Datenschutzgrundverordnung gilt in Deutschland wie bisher das sogenannte **Verbotsprinzip**: Jede Verarbeitung personenbezogener Daten ist zunächst **verboten**, solange sie nicht ausnahmsweise **erlaubt** ist. Diese Erlaubnis kann auf ganz unterschiedliche Weise zustande kommen und zwar:

Wann ist die Weiterverarbeitung zulässig?

- bei einer Einwilligung der betroffenen Person,
- wenn die Verarbeitung im Tarifvertrag oder durch eine Betriebsvereinbarung vorgesehen ist,
- wenn die Verarbeitung für einen Vertrag, der von der betroffenen Person gewünscht wird, erforderlich ist,
- um einen Vertrag mit der betroffenen Person zu erfüllen,
- wenn durch gesetzliche Vorschriften eine Pflicht zur Datenverarbeitung besteht,
- wenn eine Abwägung der berechtigten Interessen des Unternehmens gegen die Interessen der betroffenen Person ergeben hat, dass das Interesse des Unternehmens überwiegt

In der Praxis bedeutet dies, dass die Verarbeitung personenbezogener Daten erlaubt ist, wenn mindestens **eine** dieser Bedingungen zutrifft. Die weitere gesetzliche Erlaubnis „Verarbeitung ist erforderlich, um lebenswichtige Interessen eines Betroffenen zu schützen“ kommt in der Praxis eines Unternehmens nur selten vor.

Prüfhinweis:
Liegt eine Einwilligung vor, die die Datenverarbeitung erlaubt?

Die Anforderungen an eine Einwilligung sind hoch. Sie muss **nach konkreter und umfassender Information** erfolgen, damit sich der Einwilligende wirklich entscheiden kann. Zudem muss sie freiwillig sein. Gerade im Arbeitsverhältnis muss für jede Datenverarbeitungseinwilligung geprüft werden, ob bei der konkreten Person oder Gruppe von Beschäftigten von Freiwilligkeit ausgegangen werden kann. Besonders in der Bewerbungsphase wird eine freiwillige Einwilligung schwer darzulegen und zu beweisen sein. Bei anderen Arbeitnehmereinwilligungen sollte der Arbeitgeber plausibel machen können, weshalb die Mitarbeiter in ihrer Entscheidung frei waren.

Prüfhinweis:
Erlaubt eine Interessenabwägung die Datenverarbeitung?

Die im Unternehmen vorzunehmende Abwägung zwischen dem Verarbeitungsinteresse des Unternehmens und dem „Geheimhaltungsinteresse" der betroffenen Person darf nicht willkürlich vorgenommen werden. Für Beschäftigte im Unternehmen ist es schwer, im Arbeitsalltag schnell und praktisch zu entscheiden, welches Interesse jeweils schwerer wiegt. Die **Generalklausel** der Interessenabwägung ist daher von Gerichten, Aufsichtsbehörden und in der juristischen Literatur in vielen Fallgruppen präzisiert worden.

- Bei bestimmten Verarbeitungen überwiegt klar das Interesse an der Datenverwendung. Zum Beispiel darf ein Unternehmen seinen Kunden Werbung per Post senden.
- Bei Verarbeitungen, die stärker in die Privatsphäre eingreifen, wird davon ausgegangen, dass stets das Interesse der betroffenen Person am Unterbleiben der Datenverwendung überwiegt (etwa eine Weitergabe detaillierter Kundenprofile).
- Jedoch gibt es Verarbeitungen, bei denen unklar oder umstritten ist, ob das „Geheimhaltungsinteresse" der betroffenen Person oder das Verwendungsinteresse des Unternehmens überwiegt. Dann **muss die Geschäftsleitung** – gegebenenfalls nach rechtlicher Beratung – **entscheiden**, ob die Datenverarbeitung vorgenommen werden darf. Eine Datenschutzaufsichtsbehörde oder ein Gericht können nachträglich überprüfen, ob richtig abgewogen wurde.

ÜBUNGSAUFGABE

Sie leiten die Personalabteilung eines mittelständischen Teekannenherstellers. Der Inhaber möchte etwas für das Betriebsklima tun und beauftragt Sie, die Geburtstage aller Beschäftigten im firmeneigenen Intranet zu veröffentlichen, „aus Datenschutzgründen“ ohne das Jahr. Sie waren gerade auf einer Datenschutzschulung und sind unsicher, ob das so in Ordnung ist. Bitte prüfen Sie, ob das Anliegen datenschutzrechtlich zulässig ist.

LÖSUNG

Ein Spezialgesetz für Geburtstagslisten gibt es natürlich nicht. Eine entsprechende Betriebsvereinbarung wird in aller Regel ebenfalls fehlen. Auch Arbeitsverträge enthalten üblicherweise keine entsprechenden Regeln. Damit lässt sich die Verteilung der Geburtstagsliste an Kollegen in den meisten Fällen nur mittels Einwilligung oder Interessenabwägung rechtfertigen (=Datenverarbeitung zulässig, wenn Interesse des Unternehmens an der Verwendung der Geburtstagsdaten überwiegt). Das Unternehmen hat typischerweise – aber durchaus nicht immer – das überwiegende Interesse, den sozialen Zusammenhalt im Interesse der betrieblichen Effizienz durch die Möglichkeit des Geburtstagsgrußes zu verbessern. Dafür ist eben die Jahresangabe nicht unbedingt erforderlich. Um klar einen Ausschlag zum Interesse der Verwendung und Verteilung der Geburtstagsliste zu geben, sollte jedem Mitarbeiter ein Widerspruchsrecht eingeräumt werden. Sie entscheiden sich aber wegen der schwierigen Interessenabwägung dafür, alle Mitarbeiter einzeln um ihre Einwilligung zu bitten.

WER SORGT FÜR GUTEN DATENSCHUTZ?

Noch einmal zur Erinnerung: Alles, was hier zu „Unternehmen“ und „Mitarbeiterinnen und Mitarbeitern“ gesagt wird, betrifft in gleicher Weise auch Vereine, Stiftungen, öffentliche und kommunale Einrichtungen sowie deren Beschäftigte, ehrenamtlich Mitarbeitende, Praktikantinnen usw.

DIE UNTERNEHMENSLEITUNG SCHAFFT DIE RAHMENBEDINGUNGEN

Das Unternehmen haftet für Datenschutzverletzungen. Die Geschäftsleitung handelt datenschutzkonform, wenn sie die Mitarbeiter dazu verpflichtet, ihre Arbeitsaufgaben datenschutzkonform zu erfüllen und datenschutzkonformes Handeln durch konkrete Arbeitsanweisungen vorgibt. Typischerweise gibt das Unternehmen dazu Weisungen zur Datenverarbeitung heraus, die sich auf den jeweiligen Arbeitsbereich beziehen, und kontrolliert deren Einhaltung. Mit diesen Anweisungen erfüllt die Unternehmensleitung als **Verantwortlicher für die Datenverarbeitung** die gesetzliche Pflicht (Art. 29 DSGVO), dass Mitarbeiter „Daten **ausschließlich auf Weisung des Verantwortlichen verarbeiten**“ dürfen. Ohne eine solche Weisung dürfen Daten nur dann verarbeitet werden, wenn es eine gesetzliche Verpflichtung dafür gibt.

Lassen die datenschutzbezogenen Arbeitsanweisungen den einzelnen Beschäftigten Handlungsspielräume, muss die Unternehmensleitung die Beschäftigten mit einer Datenschutzanweisung nach DSGVO informieren. Diese Datenschutzanweisung enthält allgemeinere Vorgaben als die datenschutzbezogenen Arbeitsanweisungen und ermöglicht es den Beschäftigten, sich im konkreteren Anwendungsfall für datenschutzkonformes Handeln zu entscheiden. Die vorliegende Broschüre ist eine solche allgemeine Datenschutzanweisung.

Darüber hinaus sollten **Vorgesetzte**, Abteilungsleiter etc. jederzeit in der Lage sein, datenschutzrelevante Anweisungen zu erteilen und Fragen zu beantworten. Auch für sie ist daher diese Broschüre hilfreich.

DIE BESCHÄFTIGTEN WENDEN DIE VORSCHRIFTEN AN

Wenn Sie in Ihrem Arbeitsalltag Daten von natürlichen Personen verarbeiten – eine solche Datenverarbeitung beginnt schon mit dem Anlegen von Adressverzeichnissen in der Bürosoftware – sind **einige Arbeitsvorgänge durch Anweisungen und/oder die IT-Systeme vorgegeben**. So sehen beispielsweise Personaldatenverarbeitungs- und Finanzbuchhaltungssysteme fast immer vor, dass nur bestimmte Daten überhaupt eingegeben und verarbeitet werden können. Auch Passwortlängen

und Passwortarten sind oft fest definiert. Wenn aber konkrete Anweisungen fehlen, müssen Sie selbst datenschutzrelevante Entscheidungen treffen. Dazu müssen Sie die Vorgaben des Datenschutzrechts kennen.

Praxisfälle

- 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?

Dazu prüfen Sie Ihr Vorgehen in zwei Schritten:

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

Prüfhinweis:
Die eigenen Pflichten

Manchmal liegt es auf der Hand, manchmal ist es unklar, ob die eigene Datenverarbeitung datenschutzrechtlich zulässig ist. Hier können Ihnen die „**Daumenregel**“ auf Seite 23 und die weiteren Erläuterungen zu den Erlaubnissen auf Seite 21 helfen. Wenn Sie unsicher sind, fragen Sie Ihren Vorgesetzten. Und wenn Sie keinen passenden Ansprechpartner erkennen, wenden Sie sich an Ihren **Datenschutzbeauftragten**. Er oder sie ist die **wichtigste Person für Datenschutzfragen im Unternehmen**.

DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE BERÄT UND PRÜFT

Das Unternehmen muss in Deutschland eine oder einen betrieblichen Datenschutzbeauftragten stellen, wenn es in der Regel 20 Personen oder mehr ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 BDSG, dort sind auch weitere Anforderungen geregelt).

Aufgabe des Datenschutzbeauftragten ist es, Geschäftsleitung und Beschäftigte hinsichtlich datenschutzkonformer Datenverarbeitung zu beraten. Gerade für Projekte mit neuen Datenverarbeitungen sollte frühzeitig das Know-how des Datenschutzbeauftragten abgefragt werden. Eventuell ist auch eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO erforderlich; nämlich dann, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Darüber hinaus überwacht der Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften einschließlich der Zuweisung von Zuständigkeiten sowie der Sensibilisierung und Schulung der Beschäftigten, und ist Anlaufstelle für die zuständige Datenschutzaufsichtsbehörde.

Die **Aufgabe, den Datenschutz sicherzustellen**, hat der Beauftragte dagegen **nicht**. Diese Aufgabe liegt bei der Unternehmensleitung und bei den Mitarbeitern.

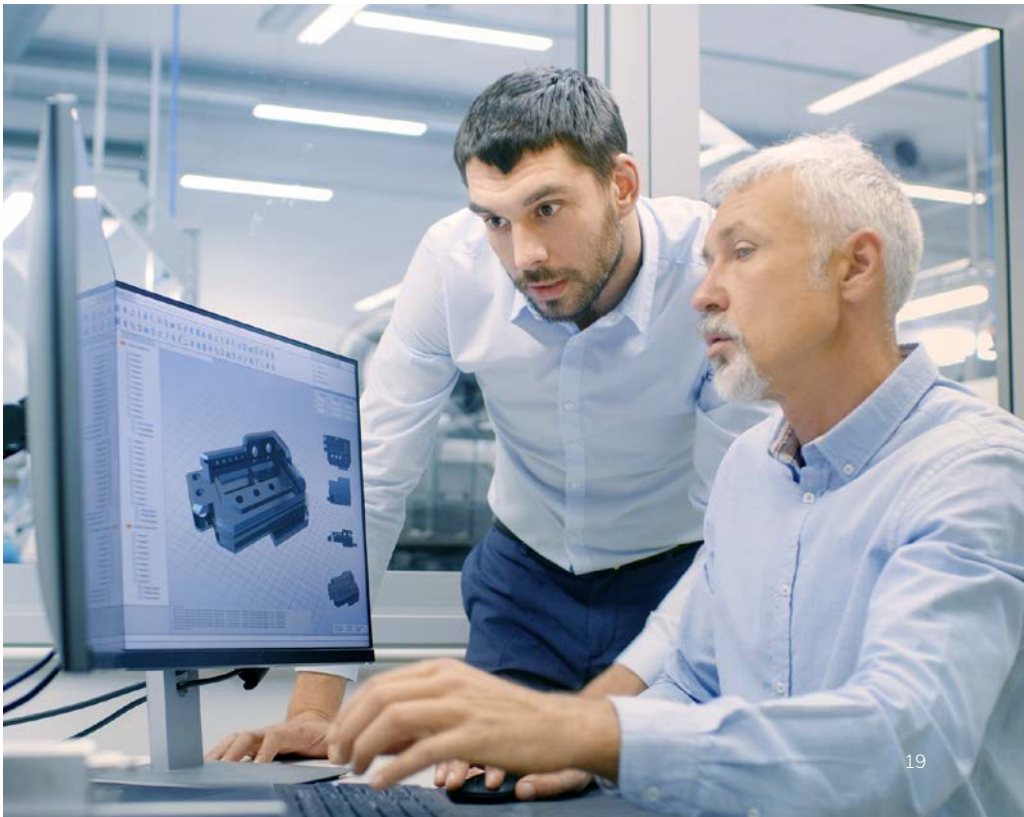
Als unabhängiger und zur Verschwiegenheit verpflichteter Kontrolleur steht der Datenschutzbeauftragte aber als Ansprechpartner für alle Beschäftigten zur Verfügung. **Jede Meldung zu datenschutzrelevanten Umständen im Unternehmen wird er vertraulich bearbeiten.** Sollten Sie Fragen zum Datenschutz haben, können Sie sich also nicht nur an Ihren 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 (in Bayern das Landesamt für Datenschutzaufsicht). Der Bundesbeauftragte für den Datenschutz ist für Bundesbehörden und für die Unternehmen der Telekommunikations- und Postbranche zuständig.

Der Bußgeldrahmen ist mit der Datenschutz-Grundverordnung erheblich erhöht worden: Schwerste Datenschutzversöße können nun mit Bußgeldern bis zu bis zu 20 Mio. Euro oder von bis zu vier Prozent des weltweiten Jahresumsatzes geahndet werden.



HINWEISE FÜR DIE PRAXIS

Wie schon im Abschnitt „Wer sorgt für guten Datenschutz?“ dargestellt, ist grundsätzlich das Unternehmen für den Schutz der personenbezogenen Daten von Personal, Bewerberinnen und Bewerbern, Kunden, Lieferanten u.ä. verantwortlich. Die Datenschutzgesetze sehen dafür die folgenden vier Pflichten vor:

- Die Pflicht zur **Erlaubnisprüfung**: Die Datenverarbeitung muss durch eine Rechtsgrundlage überhaupt erlaubt sein.
- Die Pflicht zur **Information**: Die Betroffenen müssen über die Verarbeitung ihrer Daten informiert sein.
- Die Pflicht zur **sicheren** Verarbeitung: Bei der Datenverarbeitung müssen die Grundsätze der Datensicherheit berücksichtigt werden.
- Die Pflicht zur **Datenlöschung**: Die Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.

Wenn Sie in Ihrem Arbeitsalltag mit personenbezogenen Daten umgehen und die Unternehmensleitung keine speziellen Arbeitsanweisungen gegeben hat, ist es Ihre Aufgabe, diese Pflichten zu befolgen. Dabei gehen Sie am besten orientiert an den Fragen in diesem Abschnitt vor.

IST DIE DATENVERARBEITUNG ERLAUBT?

An erster Stelle steht die **Erlaubnisprüfung** (siehe auch Abschnitt „Rechtliche Grundlagen“). Ohne dass eine der gesetzlichen Erlaubnisse erfüllt ist (**Einwilligung, Rechtsvorschrift, Betriebsvereinbarung, Vertrag oder Vertragsvorbereitung auf Wunsch des Kunden, überwiegendes Interesse des Unternehmens ist**), darf das Unternehmen keine personenbezogenen Daten verarbeiten. Entscheidend ist dabei immer, ob die Kundendaten auch tatsächlich erforderlich sind, um den konkreten Zweck zu erreichen: Für den Brötchenkauf beim Bäcker um die Ecke sind keine personenbezogenen Daten erforderlich, wenn bar bezahlt wird; ein Car-Sharing-System funktioniert dagegen ohne Datenerhebung nicht (schon allein zu Abrechnungszwecken und zur Zuordnung von Verkehrsverstößen ist die Speicherung einiger Daten zur fahrenden Person notwendig).

Beispiele für erlaubte Datenverarbeitung

- Kundenname und Kundenadresse sowie Geburtsdatum und Bankdaten dürfen verwendet werden, um einen **Online-Einkauf** des Kunden auf Rechnung mit SEPA-Lastschrift durchzuführen. Es darf dann zudem

die E-Mail-Adresse gespeichert werden; auch, um den Kunden **Newsletter** über eigene ähnliche Waren oder Dienstleistungen zu senden und damit Direktwerbung zu betreiben. Unverzichtbar ist es dann allerdings, neben den allgemeinen Informationen (siehe Antworten auf die zweite Frage „Ist die betroffene Person über die Datenverarbeitung informiert?“) auch die Information über das Werbewiderspruchsrecht zu geben.

- Die Personalabteilung darf **Lebensläufe und Zeugnisse** für Zwecke der Einstellung und der Personalverwaltung verarbeiten (Erlaubnisgrund: Entscheidung über die Begründung eines Beschäftigungsverhältnisses und Durchführung oder Beendigung eines Beschäftigungsverhältnisses nach Sondervorschrift des § 26 Abs. 1 Satz 1 BDSG als spezifischere Regelung zu Art. 6 Abs. 1 Satz 1 Buchstabe b DSGVO).
- Die Buchhaltung muss **Reisekostenabrechnungen** von Bewerberinnen und Bewerbern in Deutschland für zehn Jahre gesondert aufbewahren, allerdings nicht die gesamte Bewerbungsakte, sondern nur die Belege (Erlaubnisgrund: Rechtsvorschrift). Der Zweck wird bei solchen Archivierungen eingefroren („gesetzliche Einschränkung der Verarbeitung“), d.h. die Daten dürfen auch für keinen anderen Zweck verwendet werden.
- Die Personalabteilung darf **Lebensläufe und Zeugnisse** von abgelehnten Bewerbern in einem Bewerberpool für spätere Stellenbesetzungen speichern, wenn die Bewerber dem zuvor zugestimmt haben (Erlaubnisgrund: Einwilligung). Die Daten sonstiger, für die konkrete Stelle abgelehnter, Bewerber müssen spätestens ein halbes Jahr nach endgültiger Besetzung entweder gelöscht/vernichtet bzw. an die Bewerber zurückgesendet werden, weil kein Erlaubnisgrund zur weiteren Datenverarbeitung besteht.
- Die Betriebsrevision darf **Beschäftigtendaten** erheben, um die korrekten Abläufe des Unternehmens zu prüfen. Dabei ist es datenschutzrechtlich geboten, im Zweifel die Daten nicht unter dem konkreten Namen, sondern unter einem Code zu erheben (pseudonymisierte Daten). Die Informationen werden dabei von den Namen getrennt (Erlaubnisgrund: Überwiegendes Interesse des Unternehmens im Rahmen der Interessenabwägung).
- Die IT-Abteilung ist befugt, zur Bereitstellung des Netzwerkverkehrs oder zur SPAM-Kontrolle eine Vielzahl von **Inhalten des Netzverkehrs** automatisiert zu prüfen und zu filtern (Erlaubnisgrund: Betriebsvereinbarung oder Interesse des Unternehmens im Rahmen der Interessenabwägung, ggf. mit Einwilligung).

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?

„Daumenregel“: Um es so einfach wie möglich zu sagen, stellen Sie sich zumindest die folgende Prüfungsfrage:

Wenn es sich um Ihre eigenen personenbezogenen Daten handeln würde, die gerade erhoben, verarbeitet oder weitergegeben werden sollen: Hätten Sie für sich selbst Bedenken?

Wenn Sie diese Frage mit „Ja“ beantworten, sollten Sie sich an Ihren Vorgesetzten oder Ihren Datenschutzbeauftragten wenden.

IST DIE BETROFFENE PERSON ÜBER DIE DATENVERARBEITUNG INFORMIERT?

Im Datenschutzrecht reicht es nicht aus, dass die Datenverarbeitung zulässig ist – die betroffene Person muss auch über die Verwendung ihrer Daten informiert sein. Sie soll klar erkennen können, dass personenbezogene Daten über sie gespeichert und verarbeitet werden. Sie soll wissen, von welchem Unternehmen und zu welchem Zweck und um welche Daten es sich handelt (Art. 12 bis 14 DSGVO). Auch ein Hinweis auf ein Widerspruchsrecht ist ein Muss.

Auch bei Alltagsgeschäften gelten die Informationspflichten: Bei telefonischen Bestellungen bietet sich etwa ein Link, der aufs Handy gesendet wird, oder die Mitteilung einer URL an, unter der der Kunde die Informationen abrufen kann. Bei vertraglich erlaubter Datenverarbeitung sollten diese Informationen schon im Vertrag stehen.

Ihre Checkliste zur Informationspflicht

Ist die betroffene Person hinreichend informiert über

- ☐ den vollständigen Namen und
- ☐ die vollständige Adresse Ihres Unternehmens,
- ☐ die vollständige Adresse des Datenschutzbeauftragten (wenn es einen gibt),
- ☐ 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,
- ☐ die zeitliche Dauer, in der die Daten ungelöscht und uneingeschränkt verwendbar im Unternehmen verbleiben,

- ☐ 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?

Der beste Datenschutz bringt wenig, wenn die **Datensicherheit** aus dem Blick gerät. Unternehmen wie Beschäftigte haben technisch vor allem dafür Sorge zu tragen, dass personenbezogene Daten **nicht abhandenkommen, nicht von Unbefugten eingesehen** und **verändert** werden können. Auch ist darauf zu achten, dass die Weitergabe, wenn sie erforderlich ist, **sicher** erfolgt. Schon durch kleine Unachtsamkeiten können Unternehmen und betroffenen Personen große Schäden entstehen, die meist nicht mehr rückgängig zu machen sind.

Beispiel für unzulässigen unsicheren Datenumgang

Sie versenden eine geschäftliche E-Mail und achten beim Versenden nicht auf den korrekten Empfänger. Bereits durch einen Klick können so Daten einen nicht berechtigten Dritten erreichen. Beachten Sie zudem, dass E-Mails an Unternehmensfremde über das normale Internet nicht ohne Transport-Verschlüsselung versendet werden. Dritte können möglicherweise Einblick in die Kommunikationsinhalte nehmen, wenn sie nicht auf dem Weg zur Empfängerin verschlüsselt sind.

Es ist daher arbeitsvertragliche **Nebenpflicht, sowohl die Informationen über natürliche Personen als auch vertrauliche Firmeninformationen vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen**. Um Pannen bei der Verwendung und Weitergabe personenbezogener Daten zu vermeiden und um sich selbst abzusichern, sollten sich Beschäftigte strikt an die entsprechenden Vorgaben der Geschäftsleitung halten. Dabei gibt es wichtige **Datensicherheitsgebote**, die **stets berücksichtigt werden müssen**.

DATENSICHERHEITSREGELN

Datenerfassung
Erfasst werden dürfen **nur für den jeweiligen Zweck erforderliche Informationen**. Ein Zuviel an personenbezogenen Daten ist rechtswidrig (siehe Abschnitt „Wann lässt das Datenschutzrecht die Verarbeitung von personenbezogenen Daten zu?"). 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. **Achtung**: Nicht jeder Aktenvernichter zerkleinert die Dokumente hinreichend klein. Zu berücksichtigen ist der DIN 66399-Standard zur Vernichtung von Datenträgern. Erkundigen Sie sich bei Ihrem Vorgesetzten oder bei Ihrem Datenschutzbeauftragten, wenn Sie nicht sicher sind.

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 auch **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 geheimhaltungsbedürftige 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. Vorgesetzte, Datenschutzbeauftragte, Service-Desk, Geschäftsleitung (siehe Abschnitt „Verhalten bei Datenlecks“).

Verschlüsselung, Passwörter
Meist geben Unternehmen entsprechende Arbeitsanweisungen heraus. Andernfalls halten Sie sich am besten an die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.bund.de) – dessen Empfehlungen übrigens 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 Name 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. Sie wird Ihre Angeben vertraulich behandeln und ist auch gegenüber der Unternehmensleitung zur Verschwiegenheit verpflichtet.

Bedenken Sie: Selbst die besten Unternehmenssicherheitsvorschriften nützen nichts, wenn sich nicht alle Beschäftigten jederzeit daran halten. Das Ziel des datensicheren Unternehmens kann nur so gut erreicht werden, wie die Umsetzung an der schwächsten Stelle ist. Und die schwächste Stelle ist der Alltag mit seinen Anforderungen. Doch wer gegen die Vorgaben handelt und beispielsweise sein Passwort unberechtigt weitergibt, kann die Sicherheit des Unternehmens erheblich beeinträchtigen und haftet für die entstehenden Schäden (siehe auch „Haftung bei Datenschutzverstößen“).

Prüffrage

Habe ich alles in meiner Macht stehende getan, dass meine für die konkrete Sache nicht zuständigen Kollegen 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 gesetzlichen Fristen** der Zugriff auf personenbezogene Daten eingeschränkt wird bzw. die betreffenden Daten gelöscht werden.

Beispiel

So ist zulässig, bestimmte Bereiche des Betriebs, wie den Eingang zum Lager, per Videokamera zu überwachen. 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 nicht dafür genutzt werden, zum Beispiel über Wochen hinweg das Kommen und Gehen einzelner Mitarbeiter zu ermitteln.

Personenbezogene Daten, die vom Unternehmen verarbeitet werden, dürfen nicht durch Beschäftigte nach Gutdünken gelöscht werden. Für das Löschen muss die Unternehmensleitung Arbeitsanweisungen herausgeben. Dazu braucht es ein **Konzept für die Datenarten und Löschungsfristen**.

Für diese Löschfristen stellt sich die Frage, **wann denn überhaupt die konkreten Daten zu löschen sind**. Das Gesetz nennt keinen konkreten Zeitraum, sondern gibt vor, dass Daten zu löschen sind, wenn sie für „**die Zwecke**, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, **nicht mehr notwendig**“ sind (Art. 17 Abs. 1 Buchstabe a DSGVO). Häufig kann die konkrete Frist daraus nur durch eine rechtliche Bewertung ermittelt werden.

Beispiel

Bewerbungsunterlagen müssen in Deutschland spätestens sechs 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 Bewerber 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 Bewerberinnen nach sechs Monaten gelöscht werden müssen, bleibt ihre Adresse auf der Reisekostenabrechnung noch für zehn Jahre in Deutschland gespeichert. Allerdings muss der Zugriff auf diese Information in dieser Zeit eingeschränkt werden, so dass ein Zugriff im Tagesgeschäft oder für andere Zwecke nicht mehr möglich ist.

Häufig können Beschäftigte persönliche Speicherbereiche (persönliches Dateiverzeichnis/Home-directory) nutzen. Diese Speicherbereiche oder -medien müssen von den Beschäftigten selbst um personenbezogene Daten bereinigt werden.

BETROFFENENRECHTE

Die Datenschutz-Grundverordnung gibt Personen, deren Daten im Unternehmen verarbeitet werden, eine Reihe von Rechten in Bezug auf diese Daten. Das sind in erster Linie Auskunfts- und Löschansprüche. Daher muss ein Unternehmen in der Lage sein, Auskunft zu erteilen, welche Daten es zu einer Person speichert, zu welchem Zweck, zur Dauer der Speicherung und zu einer eventuellen Datenweitergabe. Neu ist das Recht auf Datenübertragbarkeit: Wenn eine Person einem Unternehmen personenbezogene Daten über sich selbst zur Verfügung stellt, dann muss das Unternehmen ihr auf Anforderung diese Daten in einem „strukturierten, gängigen, maschinenlesbaren und interoperablen Format“ bereitstellen oder auf ihren Wunsch an einen anderen Anbieter übermitteln (Art. 20 DSGVO).

FAZIT

LÖSCHEN VON PERSONENBEZOGENEN DATEN

Für Sie folgt aus dem Gesetz **nur in Ausnahmefällen eine eigene Pflicht**, personenbezogene Daten im Unternehmen zu löschen. Nämlich dann, wenn Sie personenbezogene Daten in eigens für Sie vorgehaltenen Bereichen speichern (USB-Sticks, eigener Server-Bereich). Im Übrigen halten Sie die **Vorgaben des Unternehmens zum Löschen** ein. Wenn Sie Fragen haben, wenden Sie sich an den Vorgesetzten oder Ihren Datenschutzbeauftragten.

Um diese Anforderungen zu erfüllen, muss die Geschäftsleitung geeignete Arbeitsanweisungen herausgeben. Die Stiftung Datenschutz hat zu diesem Betroffenenrecht eine eigene Broschüre für Unternehmen veröffentlicht[3].

DATENVERARBEITUNG DURCH DIENSTLEISTER – AUFTRAGSVERARBEITUNG

In der arbeitsteiligen Wirtschaft ist es unvermeidlich, dass Unternehmen personenbezogene Daten an Zulieferer und sonstige Dienstleister (wie Aktenvernichtungsunternehmen, Rechenzentren, IT-Dienstleister, Cloud-Computing-Anbieter usw.) zur Bearbeitung weitergeben, sei es aktiv durch Übersendung oder passiv durch Einräumen von Zugriffsrechten. Hier schreibt der Gesetzgeber einen Vertrag vor, der den **Dienstleister und dessen Beschäftigte verpflichtet, die gesetzlichen Datenschutzregelungen einzuhalten**. Dabei bleibt der Auftraggeber weiterhin für den datenschutzkonformen Umgang mit den Daten verantwortlich; der Auftraggeber ist auch verpflichtet zu prüfen, ob die Vorgaben eingehalten werden. Dies wird als Auftragsverarbeitung bezeichnet.

Kann ein Dienstleister frei entscheiden, **welche** personenbezogenen Daten im Auftrag **wie** verarbeitet werden (das betrifft üblicherweise Rechtsanwälte, Betriebsärzte oder Banken), muss geprüft werden, ob für die Übermittlung an diese Dienstleister ein Erlaubnistatbestand zutrifft (siehe Abschnitt „Wann lässt das Datenschutzrecht die Verarbeitung von personenbezogenen Daten zu?“). Auch hier ist ein Vertrag erforderlich, und es dürfen die personenbezogenen Daten durch den Dienstleister nur zweckgebunden verwendet werden.

Checkliste Auftragsverarbeitung

Schon bei der Nutzung einer Web- oder Smartphone-App kann es sich um Auftragsverarbeitung von Daten handeln. Prüfen Sie daher, wenn Sie für die Beauftragung von Dienstleistern zuständig sind und Dienstleister mit personenbezogenen Daten des Unternehmens zu tun haben, ob ein **Datenschutzvertrag** mit bestimmten, gesetzlich vorgegebenen Inhalten vorliegt. Dann müssen neben dem Vertrag vorliegen:

- ☐ eine Datensicherheitsbeschreibung
- ☐ ein Kontrollverfahren für den Dienstleister durch hinreichend plausible Datensicherheitsbewertungen oder eigene Kontrollen
- ☐ eine Dokumentation der Zuverlässigkeitseinschätzung.

Der Datenschutzbeauftragte, so vorhanden, kann weiterhelfen.

3 https://sds-links.de/datenportabilitaet

DATENVERARBEITUNG IM AUSLAND

Innerhalb des Europäischen Wirtschaftsraums (Europäische Union sowie Island, Liechtenstein und Norwegen) ist durch die Europäische Datenschutz-Grundverordnung (DSGVO) und Vereinbarungen ein einheitlicher Datenschutzstandard geschaffen. Hier sind einfach nur die Regeln dieser Arbeitsanweisung der Geschäftsleitung zum Umgang mit personenbezogenen Daten nach DSGVO anzuwenden.

Häufig werden jedoch auch Rechenzentren, Software- und Cloud-Computing-Anbieter genutzt, die ihren Sitz außerhalb des Europäischen Wirtschaftsraums haben (Drittländer). Damit durch den Transfer in diese Länder die europäischen Datenschutzstandards nicht verletzt werden, verpflichtet die DSGVO die datenempfangenden Unternehmen in Drittländern zu besonderen Maßnahmen. Fragen Sie Ihre Vorgesetzten und – so vorhanden – die oder den Datenschutzbeauftragten nach konkreten Arbeitsanweisungen. Bereits ein internationaler Datenschutzvertrag mit bestimmten Inhalten kann diese Rechtfertigung darstellen. Es ist in der Regel Sache der Rechtsabteilung oder des Rechtsanwalts Ihres Unternehmens, die notwendigen Verträge zu erstellen. Der Datenschutzbeauftragte hat dabei zu beraten und die Umsetzung zu kontrollieren.

FAZIT

DATENÜBERTRAGUNG INS AUSLAND

Fehlt die Rechtfertigung eines Datenflusses in Länder außerhalb des Europäischen Wirtschaftsraums, kommt es zu einer Datenschutzverletzung. Fällt Ihnen ein solcher Datentransfer auf, informieren Sie Ihren Vorgesetzten und gegebenenfalls den Datenschutzbeauftragten.

VERHALTEN BEI DATENLECKS

Kein Unternehmen ist 100%ig sicher; in jedem Unternehmen wird es irgendwann einmal einen „Datenschutzvorfall“ geben. So können beispielsweise digitale Speichermedien, wie ein USB-Stick oder die Speicherplatte in einem ein Laptop, verlorengehen oder es kann zu einem Einbruch auf dem Webserver oder direkt in den Serverraum kommen. Das Wichtigste, was dann zu tun ist: Etwaigen Schaden von den betroffenen Personen (deren Informationen abhandengekommen sind) und vom Unternehmen abzuwenden.

Damit solche Vorfälle nicht verheimlicht werden, schreibt der Gesetzgeber vor, dass zum Schutz der betroffenen Personen **ein Datensicherheitsvorfall zumindest der zuständigen Datenschutzaufsichtsbehörde und gegebenenfalls den betroffenen Personen gegenüber bekannt gemacht werden muss**. Wird etwas verschwiegen und später aufgedeckt, ist mit erheblichen Nachteilen und Strafen zu rechnen.

Doch **wann** muss der Aufsichtsbehörde ein solcher Datensicherheitsvorfall **gemeldet werden**? Eine Meldepflicht besteht immer, es sei denn, der Vorfall führt „nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen“. Ob das zutrifft, können meist nur Fachleute beurteilen. **Wenn Sie also einen Datensicherheitsvorfall erkennen, wenden Sie sich sofort an Ihren Vorgesetzten und an den betrieblichen Datenschutzbeauftragten.**

Die Meldung an die Aufsichtsbehörde muss **innerhalb von 72 Stunden erfolgen**, nachdem ein Angehöriger des Unternehmens oder der Einrichtung den Vorfall entdeckt hat. Die Frist beginnt sofort – nicht erst, wenn die Unternehmensleitung von dem Vorfall erfahren hat. Nur in Ausnahmefällen kann diese Meldefrist überschritten werden. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr

eine Begründung für die Verzögerung beizufügen.

Verursacht der Vorfall gar ein „hohes Risiko für die Rechte und Freiheiten der betroffenen Personen“, müssen auch diese Personen benachrichtigt werden. Auch hier obliegt die Entscheidung, ob ein solches Risiko vorliegt der Unternehmensleitung; bei dieser Bewertung berät der Datenschutzbeauftragte.

Aber auch nicht meldepflichtige Vorfälle sind sorgfältig zu dokumentieren und zu analysieren, damit sie sich nicht wiederholen. Diese Aufgaben obliegen der Geschäftsleitung oder den von ihr damit beauftragten Mitarbeitern und dem Datenschutzbeauftragten.

Ihre Vorgehensweise bei einer Datenschutzverletzung

Was müssen Sie tun, wenn Ihnen oder Kollegen ein Laptop, ein Tablet, ein Smartphone, ein Speicherstick, Memos oder Akten mit personenbezogenen Daten usw. abhandengekommen sind? Erstellen Sie **einen kurzen Bericht** (Welche Daten sind abgeflossen oder waren im Zugriff? Wie ist es dazu gekommen? Welche Folgen vermuten Sie?) und senden Sie diesen **an Ihren Vorgesetzen und den betrieblichen Datenschutzbeauftragten**. Der Bericht kann natürlich auch von Ihrem Vorgesetzten auf ihre mündliche Mitteilung hin erstellt werden.

Ein Datenschutzvorfall kann passieren. Wichtig sind dann allerdings Abhilfemaßnahmen. Und für Ihre Situation ist wichtig, dass Sie jederzeit nachweisen können, dass Sie Ihre Meldepflicht gegenüber dem Unternehmen erfüllt haben. Es muss also dokumentiert werden, was passiert ist, damit die notwendigen Maßnahmen ergriffen und der Aufsichtsbehörde gegenüber belegt werden können. Wie ein solcher Vorfall in Zukunft verhindert werden kann, muss dann beispielsweise durch eine Betriebsvereinbarung oder per Arbeitsanweisung geregelt werden.

HAFTUNG BEI DATENSCHUTZVERSTÖßEN

Wie schon in Abschnitt „Wer sorgt für guten Datenschutz?“ ausgeführt, haftet grundsätzlich das Unternehmen, wenn es zu Datenschutzverstößen kommt. Es drohen verschiedene Sanktionen. So kann die Aufsichtsbehörde hohe Bußgelder verhängen, wenn ein Unternehmen einen Datenschutzverstoß nicht meldet (siehe Abschnitt „Verhalten bei Datenlecks“). In Verbindung mit dem deutschen Anpassungsgesetz zur EU-Datenschutzgrundverordnung (BDSG) kann sich auch eine Haftung für die Unternehmensleitung, d.h. für den Geschäftsführer persönlich ergeben.

Auch Dritte, wie Mitarbeiter oder Kunden, können Datenschutzverstöße an die Behörde melden und damit einen Haftungsfall auslösen.

In diesem Abschnitt wird die Haftung von Beschäftigten betrachtet.

HAFTE ICH GEGENÜBER MEINEM ARBEITGEBER BEI DATENSCHUTZVERSTÖSSEN?

Eines sei vorweg festgestellt: Als Angestellter oder Arbeiter müssen nicht erster Linie Sie persönlich für Ihren Fehler einstehen, sondern das Unternehmen. Doch wenn Sie einen Datenschutzvorfall schuldhaft herbeigeführt haben, kann es – je nach Art Ihres Verschuldens – sein, dass Sie neben dem Unternehmen haften und schadensersatzpflichtig werden.

Die sogenannte beschränkte Arbeitnehmerhaftung in Deutschland schafft für Sie als Mitarbeiterin Vorteile. Für leicht fahrlässige rechtswidrige Datenverarbeitungen müssen Sie dem Arbeitgeber gegenüber nicht einstehen. Handeln Sie allerdings sehr nachlässig oder sogar absichtlich, dann nähert sich Ihre Haftung mit Zunahme Ihres Verschuldens

einer Vollhaftung an. Unabhängig von dieser Schadensersatzhaftung können Sie von disziplinarischen, behördlichen oder gerichtlichen Maßnahmen getroffen werden. Für gesetzwidriges Verhalten sind Sie, wenn Sie anders hätten handeln können, dem Arbeitgeber gegenüber also auch persönlich verantwortlich.

ARBEITSRECHTLICHE FOLGEN

Der Arbeitgeber muss kontrollieren, ob die Mitarbeiter die Datenschutzvorschriften einhalten. Bei Verstößen muss er disziplinarische Maßnahmen in Betracht ziehen. Diese Maßnahmen können eine Ermahnung, eine Abmahnung oder eine Strafversetzung sein; in schwerwiegenden Fällen kann es zu einer Kündigung oder gar außerordentlichen Kündigung kommen. Der Arbeitgeber darf Datenschutzverletzungen nicht „auf die leichte Schulter nehmen"; sonst würde er sich selbst dem Risiko eigener behördlicher Sanktionen, wie Ermittlungen, Abhilfemaßnahmen und Bußgeldern aussetzen.

Beispiele

Einer Bankmitarbeiterin wurde zulässigerweise außerordentlich gekündigt, weil sie Kontodaten eines Kunden telefonisch an eine Ausländerbehörde weitergegeben hatte.

Die Nutzung der Kundendatenbank einer Bank durch einen Bereichsleiter, um privat Kontakt zu der Kundin aufzunehmen, führte zu einer außerordentlichen Kündigung, die erst von einem Gericht auf eine Abmahnung zurückgestuft worden ist.

BUSSGELDER

Wenn Sie als Beschäftigter persönlich gegen Datenschutzpflichten verstoßen haben, kann die zuständige Aufsichtsbehörde ein Ordnungswidrigkeitsverfahren gegen Sie einleiten. Solch ein Verfahren beginnt – wie bei einer Verkehrsordnungswidrigkeit – damit, dass Sie von der Aufsichtsbehörde angeschrieben werden. Man gibt Ihnen die Möglichkeit, Ihr Vorgehen zu erklären. Steht dann ein Verstoß fest, kann die Aufsichtsbehörde ein Bußgeld aussprechen.

Beispiele

Aufsehen erregt hat der Fall einer Mitarbeiterin in Bayern, die fahrlässig eine Vielzahl von Kundenadressen offen ins CC-Feld einer E-Mail eingefügt und eine Kundeninformation verschickt hatte. Damit wurden sämtlichen Kunden die E-Mail-Adressen aller anderen Kunden des Unternehmens bekannt, was klar datenschutzwidrig war. Die Beschäftigte erhielt – unabhängig von disziplinarischen Maßnahmen des Unternehmens – ein Bußgeld von der Bayerischen Aufsichtsbehörde auferlegt.

Ähnliche bekanntgewordene Fälle sind der Versand von Personaldaten über

einen Freemail-Account (web.de, gmx.de o.ä.) zur Bearbeitung zu Hause oder die für private Zwecke über eine Unternehmensdatenbank eingeholte Bonitätsauskunft über eine andere Person.

GELD- UND FREIHEITSSTRAFE

Manche Datenschutzverstöße sind sogar mit Geld- und Freiheitsstrafen bedroht. Bei einem strafrechtlich sanktionierten Verstoß gegen die Anforderungen zulässiger Datenverarbeitung droht Ihnen als Beschäftigtem ein Strafverfahren. Bereits das unbefugte Löschen einer E-Mail oder die unbefugte Weitergabe von Dokumenten eines Kollegen kann unter bestimmten Voraussetzungen eine Straftat darstellen. Häufig muss für die Strafbarkeit allerdings eine Schädigungsabsicht oder eine Bereicherungsabsicht gegeben sein.

Beispiel

Das heimliche Anbringen von GPS-Geräten an einem Fahrzeug zur Ermittlung des Bewegungsprofils einer Person ist strafbar, wenn es gegen Entgelt erfolgt.

FAZIT

HAFTUNG

Datenschutzverstöße durch Mitarbeiter im Unternehmen können Schadensersatzpflichten und Bußgelder nach sich ziehen, im Extremfall sogar strafrechtliche Verurteilungen. Schadensersatzpflichten können bei hohem persönlichen Verschulden neben dem Unternehmen auch den Mitarbeiter treffen, der den Verstoß begangen hat. Zudem drohen ihm arbeitsrechtliche Konsequenzen bis hin zur außerordentlichen Kündigung.

FÜR IHRE NOTIZEN

Ergänzend zu „Datenschutz im Betrieb – Eine Handreichung für Beschäftigte“ hat die Stiftung Datenschutz auch die Broschüre „Datenschutz ganz kurz – Was Beschäftigte unbedingt wissen sollten“ veröffentlicht (DIN lang, 20 Seiten).

Diese fasst die wichtigsten Punkte praxisorientiert und leicht verständlich zusammen, und soll betriebliche Anweisungen zum Umgang mit personenbezogenen Daten unterstützen. *(Die Hinweise gelten genauso für Vereine und andere Organisationen.)* Beide Versionen sind auch in englischer Sprache verfügbar. Alle Versionen können über die Website stiftungdatenschutz.org abgerufen werden.

Herausgeber
Stiftung Datenschutz

Version
2.1, Stand März 2020

Autor
Dr. Philipp Kramer

Über den Autor
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.

ÜBER DIE STIFTUNG DATENSCHUTZ

Die STIFTUNG DATENSCHUTZ wurde 2013 von der Bundesrepublik Deutschland gegründet. Die unabhängige Einrichtung dient als Informationsplattform zur Umsetzung des Datenschutzrechts und als Diskussionsplattform zur Datenpolitik. Die Bundesstiftung fördert den Dialog zwischen Gesellschaft, Politik, Wirtschaft und Forschung. Die STIFTUNG DATENSCHUTZ ergänzt als neutraler Akteur die Datenschutzaufsichtsbehörden in Bund und Ländern.

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
Frederick Richter (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 BMJ).

Bundesministerium der Justiz