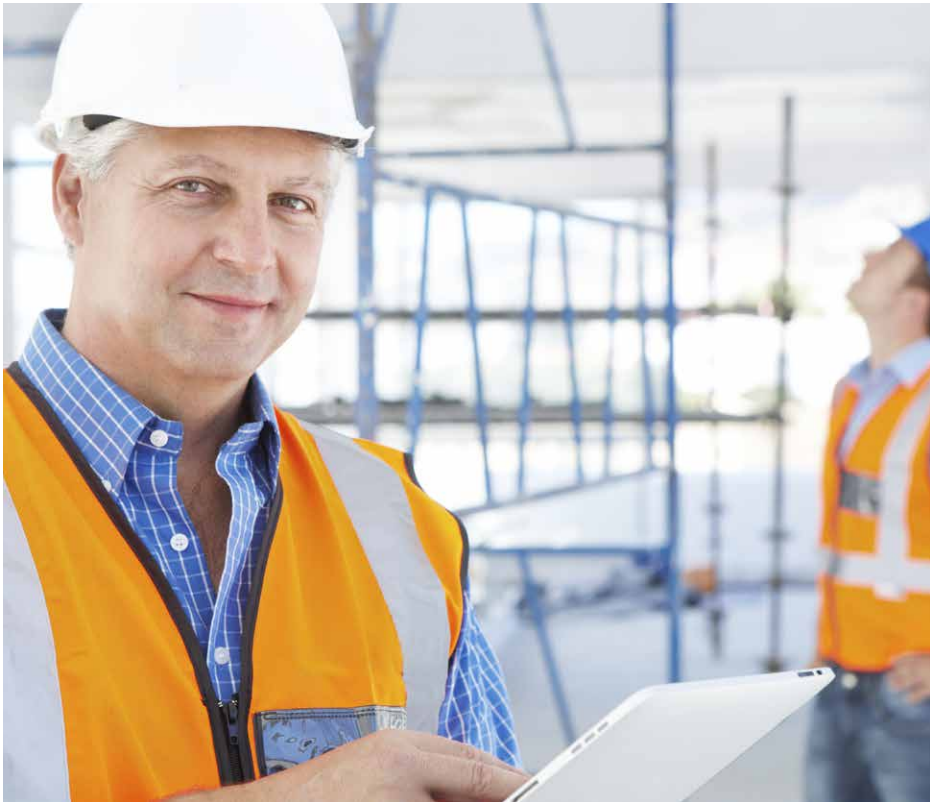


DATENSCHUTZ IM BETRIEB

EINE HANDREICHUNG FÜR BESCHÄFTIGTE IN KLEINEN UND MITTELSTÄNDISCHEN UNTERNEHMEN

STIFTUNG DATENSCHUTZ

INHALT

FÜR WEN IST DIESE BROSCHÜRE GEDACHT?

Für Sie als 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 dem Datenschutz nur die Unternehmensleitung, die Rechtsabteilung und der betriebliche Datenschutzbeauftragte befassen. Dazu kommen Unternehmenseinheiten, die intensiv mit personenbezogenen Daten umgehen, wie die Personalabteilung oder die Kundenbetreuung. Doch in der heutigen Arbeitswelt trifft nahezu jeder Beschäftigte für das Unternehmen auch eigene Entscheidungen zur Datenverarbeitung, bei denen er gesetzliche Vorgaben zu beachten hat.

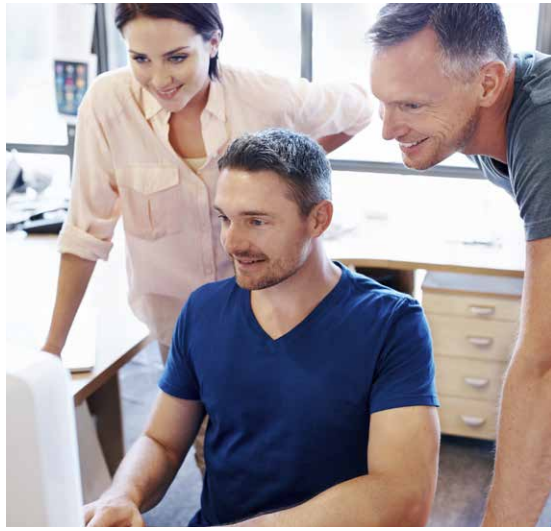
Verstoßen Sie gegen Pflichten oder handeln Sie schlicht nicht sorgfältig genug beim Datenumgang, drohen Sanktionen und nachteilige Folgen. Auch wenn Sie nur gelegentlich mit personenbezogenen Daten, zum Beispiel Kundendaten, arbeiten, müssen Sie die gesetzlichen Regelungen kennen und beachten. Dabei will Ihnen diese Broschüre helfen. Unter Umständen hat Ihre Geschäftsleitung aufgrund spezifischer Anforderungen in Ihrem Betrieb zusätzliche Arbeitsanweisungen erlassen.

Als Beschäftigter erhalten Sie typischerweise immer Informationen über Kollegen, Kunden, Interessenten oder sonstige Ansprechpartner des Unternehmens. Sie befassen sich dann mit deren personenbezogenen Daten und übernehmen dafür auch Verantwortung. Kennen Sie Ihre wesentlichen Datenschutzpflichten nicht, drohen Ihnen auch bei unbewusstem Fehlverhalten Sanktionen und nachteilige Folgen. Denn auch beim Datenschutz kann man sagen: „Unwissenheit schützt vor Strafe nicht!“. Beachten Sie die nachfolgende Instruktion zum Datenschutz, die zugleich generelle Arbeitsanweisung/Dienstanweisung Ihres Arbeitgebers sein kann.

Für jedes Unternehmen, das mit personenbezogenen Daten umgeht und daher seine Beschäftigten über Datenschutz informieren muss.

Als Unternehmensleitung sind Sie verpflichtet, Ihre Belegschaft zum Datenschutz aufzuklären. Das bedeutet: Die Beschäftigten müssen wissen, was sie mit personenbezogenen Daten am Arbeitsplatz machen dürfen und was nicht. Um die notwendige Grundinformation durchzuführen, kann das Unternehmen Handreichungen wie diese unmittelbar einsetzen.

Die Broschüre kann die konkreten Dienstanweisungen des Unternehmens zum Umgang mit bestimmten Datenarten für bestimmte Zwecke nicht ersetzen und ist daher ggf. durch weitere Arbeitsanweisungen, beispielsweise zum Umgang mit Daten bei Direktmarketingmaßnahmen/auf mobilen Geräten/mit Daten im Home Office usw. zu ergänzen. Die Broschüre liefert jedoch die gesetzlich vorgesehene Grundinformation und allgemeine datenschutzbezogene Arbeitsanweisungen. Zu einer ersten Einführung der Belegschaft in das Thema können Sie diese Broschüre unmittelbar einsetzen.



Für Sie als betrieblichen Datenschutzbeauftragten eines Unternehmens.

Als betrieblicher Datenschutzbeauftragter müssen Sie „die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut […] machen“ (§ 4g Abs. 1 Satz 4 Nr. 2 Bundesdatenschutzgesetz). Hierzu können Sie Präsenz- oder Onlineschulungen anbieten, aber auch schriftliche Informationen wie diese Broschüre einsetzen.

WESHALB BIN AUCH ICH ALS BESCHÄFTIGTER FÜR DEN DATENSCHUTZ MEINES UNTERNEHMENS MITVERANTWORTLICH?

Weil Sie als Beschäftigter des Unternehmens Datenschutzpflichten haben, die unmittelbar Sie treffen. Diese Pflichten treten neben die Datenschutzpflichten, die schon für das Unternehmen als solches gelten.

Pflichten des Unternehmens

Ihr Unternehmen geht bei der Erstellung von Produkten und Leistungen für die Unternehmenskunden mit einer Vielzahl von Informationen um, die durch Datenschutzvorschriften geschützt sind. Der Gesetzgeber nimmt diesen Schutz derart ernst, dass er für jedweden Umgang mit solchen Informationen eine Erlaubnisvorschrift verlangt. Er nennt diese geschützten Informationen personenbezogene Daten und meint damit alle Informationen, die Kollegen, Bewerber, Verbraucher, Beschäftigte von Kunden- und Lieferanten, Gäste und andere Menschen betreffen.

Was ist geschützt?
Zu den personenbezogenen Daten gehören natürlich zunächst die Stammdaten einer Person, wie Name, Geburtsdatum, Adresse, Telefonnummer und elektronische Kontaktdaten. Weiter erfasst sind unter anderem Bankdaten, Vermögenslage, Kontakte zu anderen Personen, das Einkaufsverhalten von Kunden, das Surfverhalten auf der Unternehmenswebsite, Gewohnheiten und Hobbies, Lebenslaufdaten und die gesundheitliche Situation.

Das Unternehmen ist datenschutzrechtlich befugt, eine Vielzahl dieser Informationen im Rahmen seiner Tätigkeit zur Erstellung von Produkten oder Lieferung von Leistungen zu verwenden.

Beispiele für befugten Datenumgang

Kundenname und Kundenadresse sowie Geburtsdatum und Bankdaten dürfen verwendet werden, um einen Einkauf des Kunden auf Rechnung mit SEPA-Lastschrift durchzuführen. Beim **Online-Einkauf** kann auch die E-Mail-Adresse gespeichert werden. Maßgebend ist immer, ob die Kundendaten erforderlich für die konkrete Maßnahme sind. Im Falle eines typischen Bargeschäfts des täglichen Bedarfs, wie des Einkaufs im Supermarkt, fehlt es an dieser Erforderlichkeit, so dass der Supermarkt allenfalls mit einer Einwilligung befugt ist, solche Kundendaten zu erheben.

Die **Personalabteilung** ist befugt, Lebensläufe und Zeugnisse für Zwecke der Einstellung und der Personalverwaltung zu verwenden. Die Daten abgelehnter Bewerber sind zu löschen, sobald sie für die Besetzung der Stelle nicht mehr erforderlich sind. Spätestens ein halbes Jahr nach Besetzung der Stelle müssen die Bewerbungsunterlagen der abgelehnten Bewerber gelöscht oder – soweit sie in Papierform vorhanden sind und eine Rückgabepflicht besteht – an die Bewerber zurückgesendet werden.

Die **Revision** Ihres Unternehmens darf Beschäftigtendaten erheben, um die korrekten Abläufe des Unternehmens zu prüfen. Doch auch hier gibt es Grenzen. Um nicht eine Vielzahl von Namensdaten zusätzlich in der Revision zu erheben, ist es datenschutzrechtlich geboten, im Zweifel die Daten nicht unter dem Namen, sondern unter einem Code/Pseudonym zu speichern (pseudonymisierte Daten). Die Codeliste wird durch die Organisationseinheit (Teil einer Abteilung) aufbewahrt, die die Liste für die Revision erstellt hat und benötigt. Nur diese Stelle des Unternehmens, nicht andere, kann daher die Namen der Beschäftigten den Prüfergebnissen zuordnen und in Verdachtsfällen weitergeben.

Die **IT-Abteilung** ist befugt, Inhalte des Datenverkehrs in den Unternehmensnetzwerken zu filtern und zu prüfen, zum Beispiel Schutz vor Schadsoftware, Viren und Spam.

Pflichten des Beschäftigten

Bei Ihrer Arbeit haben Sie vielerlei Umgang mit Informationen von Kollegen, Kunden, Lieferanten, Besuchen, Bürgern usw. Viele dieser Verarbeitungsvorgänge sind fest geregelt und dann auch meist datenschutzkonform ausgestaltet. Ansonsten aber sind Sie als konkret Handelnder in der Pflicht, die Datenschutzregeln zu kennen und bei Ihrer Aufgabenerfüllung für das Unternehmen auch einzuhalten. Auch bei fertig eingerichteten IT-Systemen sollten Sie sich stets noch einmal kurz fragen, ob Ihre Eingaben datenschutzkonform sind; dies gilt vor allem in Freitextfeldern (siehe dazu Daumenregel, Seite 19).

Nach Möglichkeit hat der Arbeitgeber Ihnen hierzu konkrete Informationen und Arbeitsanweisungen zukommen lassen. Zudem sind Sie kraft Gesetzes auf den Datenschutz zu verpflichten.
Der hierzu maßgebliche § 5 Bundesdatenschutzgesetz lautet:

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Ein Muster für eine derartige Verpflichtungserklärung für Beschäftigte finden Sie in der Anlage auf Seite 32.

Beispiele für eigenverantwortliche Datenschutzentscheidungen des Beschäftigten:

Beschäftigte mit Computerzugang müssen bestimmte Sicherheitsvorgaben einhalten, die mit der ordnungsgemäßen Geheimhaltung des Passwortes beginnen.

Vorgesetzte, Betriebsratsmitglieder und Beschäftigte der **Personalabteilung** erhalten besonders sensible Informationen über Kollegen und Bewerber. Hier gelten strengere Geheimhaltungspflichten, auch und gerade gegenüber den Kollegen.

In **Marketing und Vertrieb** erhalten die Beschäftigten Informationen über Verbraucher und/oder Ansprechpartner von Kunden und Interessenten. Auch das Verbraucher- und Kundenvertrauen ist durch das Datenschutzrecht geschützt. Die Betroffenen erwarten, dass Sie sich als Beschäftigte des Marketing-/Vertriebsbereichs mit den Datenschutzpflichten des Gesetzes auskennen und danach handeln. Das muss auch in Gesprächen zum Ausdruck kommen.

Beschäftigte der **Revision** erhalten bei ihren Untersuchungen nicht nur pseudonyme Daten, sondern auch konkrete Beschäftigten-, Kunden- und Lieferantendaten.

In der **Informationstechnik/EDV** sind die Administratoren dafür zuständig, dass die IT und Ihre Anwendungen zuverlässig laufen. Ein Zugriff auf Nutzerdaten kann im Rahmen von deren Aufgabenerfüllung nicht immer auszuschließen sein. Wenn also technisch erforderlich auf E-Mail-Inhalte und Logprotokolle zugegriffen wird, muss sich der IT-Beschäftigte mit den Grenzen und Pflichten bei solchen Zugriffen genau auskennen. Und wenn andere Personen des Unternehmens von ihm Einsicht in E-Mails oder Protokolle verlangen, muss er wissen, was er darf und was ihm verboten ist.

Über die Verpflichtungserklärung hinaus müssen Sie von der Unternehmensleitung weitergehende Informationen zum Datenschutz erhalten. Soweit Ihr Unternehmen einen Datenschutzbeauftragten bestellt hat, hat dieser Sie „durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen“ (§ 4g Abs. 1 Satz 4 Nr. 2 Bundesdatenschutzgesetz).
Dazu kann der Beauftragte auch diese Broschüre einsetzen. Wenn es keinen Datenschutzbeauftragten gibt, muss der Arbeitgeber selber Sie informieren. Auch er kann diese Broschüre verwenden, um notwendiges Datenschutzwissen für die Tätigkeit im Unternehmen zu vermitteln.

Als Beschäftigter treffen Sie an verschiedenen Stellen eigenverantwortlich Datenverarbeitungsentscheidungen. Dabei sollten Sie unmittelbar das Gesetz und konkretisierende Arbeitsanweisungen beachten. Daher müssen Sie die wichtigen Regelungen des Datenschutzrechts kennen, die in dieser Broschüre aufgelistet sind.

HAFTE ICH GEGENÜBER MEINEM ARBEITGEBER BEI DATENSCHUTZVERSTÖSSEN?

Eines sei vorweg festgestellt: Nicht Sie selber müssen in erster Linie für Ihre Fehler beim Datenschutz nach außen einstehen, sondern Ihr Unternehmen. Für leichte Fehler bei der Datenverarbeitung haften Sie dem Arbeitgeber gegenüber finanziell nicht. Anders sieht es dagegen aus, wenn Sie sehr nachlässig oder sogar absichtlich gehandelt haben.

Als Beschäftigter sind Sie bei Ihrer Arbeit – je nach Branche oft oder sogar immer – an Datenverarbeitungen Ihres Unternehmens/Arbeitgebers beteiligt. Deshalb ordnet die Rechtsprechung dem Unternehmen einen Teil Ihrer Fehler zu. Wenn Sie einen Schaden verursachen, kann es aber sein, dass Sie neben dem Unternehmen haften und damit ebenfalls schadensersatzpflichtig sind. Der Umfang dieser Haftung bemisst sich für Sie als Beschäftigten – auch für in Leiharbeitsverhältnissen stehende Arbeitnehmer – nach den Grundsätzen der sogenannten „beschränkten Arbeitnehmerhaftung“:

- Normalerweise haften Sie für Schäden, die Sie verursachen, schon dann, wenn Sie die einfache gebotene Sorgfalt außer Acht gelassen haben. Durch die beschränkte Arbeitnehmerhaftung stehen Sie bei Pflichtverletzungen im Arbeitsverhältnis jedoch für einen Schaden immer nur dann voll ein, wenn Sie mit Ihrem Willen oder zumindest mit Ihrem Wissen eindeutig einen Datenschutzverstoß begangen haben. Man spricht von vorsätzlichem Handeln.

- Demgegenüber sind Sie als Beschäftigter ausnahmsweise frei von Schadensersatzpflichten, wenn Ihnen ein Fehler passiert, der auch jedem Ihrer Kollegen hätte passieren können, bei so genannter leichter Fahrlässigkeit (Beispiel: Sie verwechseln eine Faxnummer und senden ein Dokument mit personenbezogenen Daten an die falsche Faxnummer und damit an einen falschen Empfänger).

- Ist Ihnen fahrlässig ein Datenschutzversehen passiert, das nach Auffassung eines Gerichts Ihren Kollegen im Zweifel nicht passiert wäre, haben Sie also das übliche Niveau von Sorgfaltspflichten vernachlässigt, dann haften Sie für diese mittlere Fahrlässigkeit mit bis zu mehreren Monatsgehältern. Handelten Sie grob fahrlässig, müssen Sie teilweise Schadensersatz leisten.

Die beschränkte Arbeitnehmerhaftung schafft für Sie als Beschäftigten also Vorteile. Für leicht fahrlässige rechtswidrige Datenverarbeitung müssen Sie dem Arbeitgeber gegenüber nicht finanziell 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 disziplinarische, behördliche oder gerichtliche Maßnahmen treffen (dazu Abschnitt „Welche weiteren Folgen können Datenschutzverstöße für die Beteiligten haben?“).

WELCHE FOLGEN KÖNNEN DATENSCHUTZ-VERSTÖSSE FÜR DIE BETEILIGTEN HABEN?

Verstößt ein Beschäftigter gegen gesetzliche Datenschutzpflichten, handelt er gesetzwidrig. Das kann – wie oben angesprochen – Schadensersatzpflichten des Unternehmens auslösen (dazu Abschnitt „Hafte ich gegenüber meinem Arbeitgeber bei Datenschutzverstößen?“). Dabei kommt es darauf an, ob sich das Unternehmen den Verstoß des Beschäftigten zurechnen lassen muss und zusätzlich selbst gegenüber dem Betroffenen haftet. Das ist vor allem dann der Fall, wenn der Arbeitgeber oder der betriebliche Datenschutzbeauftragte die Beschäftigten nicht hinreichend darüber aufgeklärt haben, wie man als Beschäftigter die Datenschutzgesetze am Arbeitsplatz einhält. Weiterhin können die Beschäftigten von disziplinarischen, behördlichen oder gerichtlichen Sanktionen betroffen sein.

Arbeitsrechtliche Folgen

Der Arbeitgeber muss kontrollieren, ob die Datenschutzvorschriften von den Beschäftigten eingehalten werden. Er hat disziplinarische Maßnahmen wie Abmahnungen in Betracht zu ziehen, wenn Sie als Beschäftigter gegen Datenschutzvorschriften verstoßen. Damit sind Sie als Beschäftigter, der im Rahmen seiner Tätigkeit Datenschutzvorschriften verletzt, disziplinarischen Maßnahmen, wie Ermahnung, Abmahnung und Kündigung, ausgesetzt.

Für Ihr gesetzwidriges Verhalten sind Sie, wenn Sie anders hätten handeln können und es für Sie vermeidbar war, dem Arbeitgeber gegenüber auch persönlich verantwortlich. Zunächst droht Ihnen eine Ermahnung, dann eine Abmahnung oder eine Strafversetzung. In schwerwiegenden Fällen kann es zu einer Kündigung oder gar außerordentlichen Kündigung kommen. Der Arbeitgeber darf Datenschutzverletzungen auch nicht „auf die leichte Schulter nehmen“. Denn dann würde er riskieren, dass ihm ein solcher Verstoß selbst zugerechnet wird. Behördliche Sanktionen, wie Ermittlungen, Abhilfemaßnahmen und Bußgelder von Aufsichtsbehörden, würden dann auch den Arbeitgeber treffen.

Beispielfälle

- eine Bankbeschäftigte wurde außerordentlich gekündigt, weil sie Kontodaten telefonisch an eine Ausländerbehörde weitergegeben hatte (LArbG Mainz, 4 Sa 772/06)
- die Nutzung der Kundendatenbank einer Bank durch einen Bereichsleiter zur privaten Kontaktaufnahme zu einer Kundin führte zu einer außerordentlichen Kündigung, die erst vom Gericht auf eine Abmahnung zurückgestuft wurde (LArbG Mainz, 10 Sa 329/11)

Behördliche Folgen

Wenn Sie als Beschäftigter gegen Datenschutzpflichten verstoßen haben, kann gegen Sie von der zuständigen Aufsichtsbehörde ein Ordnungswidrigkeitsverfahren eingeleitet werden. Dabei würde die Aufsichtsbehörde Sie zunächst persönlich anschreiben und Ihnen die Möglichkeit geben, Ihr datenschutzwidriges Verhalten zu erklären. Steht der Verstoß fest, kann die Aufsichtsbehörde ein Bußgeld aussprechen.

Beispielfall

Aufsehen erregt hat der Fall einer Beschäftigten in Bayern, die fahrlässig eine Vielzahl von Kundenadressen offen in das CC-Feld einer von ihr verschickten E-Mail-Nachricht eingefügt hatte. Auf diese Weise wurden allen Kunden die E-Mail-Adressen aller anderen Kunden des Unternehmens bekannt, was datenschutzwidrig war. Die Beschäftigte erhielt – unabhängig von unternehmensinternen Maßnahmen – auch noch ein Bußgeld von der Bayerischen Aufsichtsbehörde auferlegt (Bayerisches Landesamt für Datenschutzaufsicht 2013).

Gerichtliche Folgen

Manche Verstöße von Beschäftigten gegen Datenschutzpflichten können sogar zu Strafverfahren führen. Bereits das unbefugte Löschen einer E-Mail oder die unbefugte Weitergabe von Dokumenten eines Kollegen kann eine Straftat darstellen.

Beispielfall
Das heimliche Anbringen von GPS-Geräten an einem Fahrzeug zur Ermittlung des Bewegungsprofils einer Person ist strafbar, wenn es gegen Entgelt erfolgt (BGH, 1 StR 32/13).

Datenschutzverstöße durch Beschäftigte im Unternehmen können Disziplinarmaßnahmen, Bußgelder und sogar strafrechtliche Verurteilungen gegen das Unternehmen nach sich ziehen. Sie können sich auch unmittelbar gegen den Beschäftigten richten, der den Verstoß begangen hat.

WARUM BETREIBT MEIN UNTERNEHMEN DATENSCHUTZ?

Sinn und Zweck des Datenschutzes

Der Datenschutz soll den Einzelnen davor schützen, dass übermäßig mit den ihn betreffenden Informationen umgegangen wird. „Datenschutz" soll nicht die Daten als solche schützen, sondern die Persönlichkeit, die hinter den Daten steht. Dem liegt die Vorstellung zu Grunde, dass jeder Mensch selbst entscheiden können soll, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Man spricht vom „Recht auf informationelle Selbstbestimmung".

Der Datenschutz ist nicht nur eine gesetzliche Vorgabe, sondern auch für die Außenwirkung Ihres Unternehmens heutzutage von hoher Bedeutung. Pannen mit Daten werden immer stärker wahrgenommen und können Kundenverhalten nachhaltig negativ beeinflussen. Fehler beim Datenumgang können nicht nur persönliche Rechte anderer Menschen verletzen, sondern infolge von Vertrauensverlusten auch handfeste wirtschaftliche Einbußen nach sich ziehen.

Geschäfts- und Betriebsgeheimnisse schützt jedes Unternehmen bereits aus eigenem Interesse. Wenn sich Daten im Unternehmen auch noch auf (natürliche) Personen beziehen, werden sie zusätzlich durch das Datenschutzrecht geschützt. Daher sind auch Informationen über Kunden, Interessenten, Besucher, und Ansprechpartner bei Lieferanten und Kunden sorgsam zu behandeln. Rechtsschutz genießen alle Daten, sobald sie „personenbezogen" sind, sobald sie also konkrete Angaben über konkrete Menschen enthalten.

Ein Personenbezug ist auch dann schon gegeben, wenn die Person zwar nicht namentlich genannt ist, der Name jedoch ermittelt werden kann. Auch solche personenbeziehbaren Daten genießen den rechtlichen Schutz.

Das gilt zum Beispiel für eine betriebsinterne Liste, auch wenn diese keine Namen enthält, sondern nur Personalnummern und andere Angaben zu den Personen. Zwar kann aus einer solchen Liste allein der Name von Personen noch nicht abgelesen werden. Doch mit einer Referenzliste, auf der sich die Beschäftigtennummer und Beschäftigtenname finden, lässt sich der konkrete Beschäftigte schnell ermitteln.

WER WIRD GESCHÜTZT UND WORUM GEHT ES BEIM DATENSCHUTZ?

Das wichtigste Gesetz in Deutschland, das den Datenschutz regelt, ist das Bundesdatenschutzgesetz (kurz BDSG). Es schützt alle Angaben zu einem Menschen wie beispielsweise Name, Anschrift, Telefonnummer oder Angaben zu Vermögensverhältnissen. Es schützt solche Informationen über Personen nicht nur dann, wenn diese Daten in Datenbanken verarbeitet werden. Es spielt keine Rolle, ob die Personendaten elektronisch (wie in einer Excel-Tabelle) oder auf Papier (wie in einer Personalakte) vorliegen. Auch eine systematisch auswertbare Word-Datei oder ein Karteikasten können genügen. Nach dem BDSG ist die Verarbeitung von personenbezogenen Daten nur erlaubt, wenn eine Vorschrift diese Verarbeitung zulässt oder wenn die Einwilligung der betroffenen Person vorliegt.

WANN DARF MEIN UNTERNEHMEN DATEN VERARBEITEN?

Typische datenschutzrechtliche Frage

Da Sie in Zukunft die Geburtstage Ihrer Kollegen nicht vergessen wollen, legen Sie eine Tabelle an, in der alle Beschäftigten des Unternehmens mit vollständigem Geburtsdatum aufgelistet sind. Diese stellen Sie in das firmeneigene Intranet, so dass jeder Kollege darauf Zugriff hat. Kollege Walter möchte aufgrund seines jugendlichen Aussehens sein wahres Alter nicht offenbaren. Kann er sich dagegen wehren oder muss er die Aufnahme in die Liste hinnehmen?

Im BDSG gilt das sogenannte Verbotsprinzip. Nach diesem Grundsatz ist jede Verarbeitung personenbezogener Daten verboten, außer sie ist durch eine Vorschrift oder eine Einwilligung erlaubt. Es ist also Sache des Unternehmens und Ihre Sache, sich vorher zu informieren, ob eine Erlaubnis durch das Gesetz oder die betroffene Person vorliegt. Vor allem im BDSG finden sich einige Regelungen, die Datenverarbeitung erlauben oder sogar anordnen. Auch in anderen Gesetzen gibt es Rechtsvorschriften, die das Unternehmen und damit die Beschäftigten der Personalabteilung und der Lohnbuchhaltung verpflichten, z. B. Lohnsteuerinformationen und Sozialversicherungsdaten aus den Beschäftigungsverhältnissen an Behörden weiterzugeben. Daneben gibt es weitere Erlaubnistatbestände, personenbezogene Daten zu verarbeiten:

- Wenn das Unternehmen Personaldaten außerhalb des Europäischen Wirtschaftsraums verarbeiten will (siehe Abschnitt „Was mache ich, wenn ich Daten in Länder außerhalb der Europäischen Union sende?“), ist es möglich, dazu eine Betriebsvereinbarung zu treffen. Gegebenenfalls müssen noch weitere Erlaubnisse für den Datentransfer in solche Länder hinzukommen.

- Wenn Verträge vorbereitet, begründet und durchgeführt werden sollen, dürfen Name und Adresse, gegebenenfalls Kontoverbindung und Lieferadresse, aufgenommen werden. Soll auf Kredit (Zahlungsziel) geliefert werden, bedarf es weiterer Informationen zur Bonität des Zahlungspflichtigen (Rechtfertigung: gegenwärtiger oder zukünftiger Vertrag).

Auch schon vor Vertragsschluss darf ein in Aussicht genommener Vertrag durch Datenerhebungen vorbereitet werden. Geht es zum Beispiel um einen Lebensversicherungsvertrag, dürfen auch Gesundheitsdaten zur Bearbeitung des Angebots erhoben und verarbeitet werden (§ 28 Abs. 6 Nr. 3 BDSG).

- Wenn das Unternehmen seine Kunden über eigene Produkte oder Leistungen bewerben will, darf es deren Adressen und gegebenenfalls weitere Informationen über den Kunden – wie seine Kaufhistorie – nutzen, um ein Postmailing aufzusetzen bis der Kunde widerspricht (Rechtfertigung: Güterabwägung: Verwendungsinteresse wiegt objektiv schwerer als Geheimhaltungsbedürfnis des Kunden an seiner Adresse).

- Geht es um Neukundenbewerbung oder um die Erhebung potentieller Bewerberdaten, darf bei einem überwiegenden Verwendungsinteresse (Güterabwägung) auf allgemein zugängliche Verzeichnisse im Internet zugegriffen werden (Rechtfertigung: öffentlich zugängliche Daten).

- Der Gesetzgeber unterstellt, dass der Betroffene ein Interesse an Werbung hat. Das Unternehmen muss demzufolge von einer Verarbeitung der konkreten Betroffenendaten absehen, wenn dieser Betroffene einen Werbewiderspruch erhoben hat (§ 28 Abs. 4 Satz 1 BDSG).

- Will ein Beschäftigter eine Firmenkreditkarte zu privaten Zwecken nutzen, ist das zulässig, wenn die entsprechende Vereinbarung vorliegt (Rechtfertigung: Vertrag / Einwilligung).

Antwort zur typisch datenschutzrechtlichen Frage (von Seite 16):

Ein Spezialgesetz für Geburtstagslisten gibt es nicht. Da das Geburtsdatum in der Regel auch nicht öffentlich zugänglich ist, eine Offenlegung der Geburtstagsinformation des Beschäftigten zur Durchführung des Arbeitsvertrags nicht erforderlich ist und eine Einwilligung des Beschäftigten im Zweifel nicht vorliegt, kann sich die Rechtmäßigkeit der Geburtstagsliste nur aus einer vom Ersteller vorzunehmenden Güterabwägung rechtfertigen.

Das Unternehmen hat, ebenso wie seine Beschäftigten, typischerweise ein hohes Interesse, den sozialen Zusammenhalt durch die Möglichkeit von Geburtstagsgrüßen zu festigen. In der Abwägung wird also regelmäßig das Interesse zur Erstellung der Liste das Interesse am Geheimhalten der Geburtstage überwiegen. Für den Zweck der Förderung des Betriebsklimas durch Glückwünsche ist allerdings keine Jahresangabe erforderlich.

Zur Zulässigkeit betriebsinterner Geburtstagslisten gibt es jedoch auch unter Fachleuten unterschiedliche Ansichten:

Teilweise wird angenommen, dass die Betroffenen ein überwiegendes Geheimhaltungsinteresse haben, teilweise eher die Auffassung vertreten, das Verwendungsinteresse des Unternehmens für ein gutes Betriebsklima sei vorrangig. So halten u. a. die Bayerische Datenschutzaufsichtsbehörde und die Bundesdatenschutzbeauftragte Geburtstagslisten für zulässig – jedenfalls dann, wenn den Beschäftigten der Einsatz der Liste angekündigt und ihnen ein Widerspruchsrecht eingeräumt worden ist. Die Thüringer und die Sächsische Datenschutzaufsicht erkennen dagegen kein berechtigtes Interesse für eine Geburtstagsliste.

Um Beschäftigte, die keine Geburtstagsgrüße wünschen, angemessen zu berücksichtigen, sollte daher in jedem Fall vor der Erstellung/Versendung ein Widerspruchsrecht eingeräumt werden, da so deren schutzwürdige Interessen gewahrt werden können.

ACHTUNG: Für die Verarbeitung von Daten in Auskunfteien und für die Verarbeitung von Gesundheits-, Religions- und weiteren sensitiven Daten gibt es Sonderregeln.

WANN VERHALTE ICH MICH ALS BESCHÄFTIGTER DATENSCHUTZKONFORM?

Als Beschäftigter können Sie täglich mit personenbezogenen Daten in Kontakt kommen. Das Unternehmen entscheidet im konkreten Fall, wie mit diesen Daten verfahren wird, im Zweifel durch Sie. Daher müssen Sie die wesentlichen Erlaubnistatbestände des Datenschutzrechts kennen (siehe Abschnitt „Wann darf mein Unternehmen Daten verarbeiten?“). Machen Sie sich ergänzend mit den beigefügten Datenschutzvorschriften (siehe Anlage: Wichtige Rechtsvorschriften, Seite 39) vertraut.

Ihre Prüffrage

Gibt es eine Vorschrift oder eine Einwilligung, die zulässt, dass ich diese Information über den Betroffenen aufbereite, weitergebe oder sonst nutze?

Daumenregel

Um es so einfach wie möglich zu sagen, stellen Sie sich zumindest die folgende Prüfungsfragen:

Würden Sie selber Bedenken haben, wenn eine Verarbeitung ihrer personenbezogenen Daten wie die konkret geplante, ohne Ihre Einwilligung erfolgen würde?

Hätten Sie für sich Bedenken, wenn es um Ihre persönlichen Daten ginge? Würden Sie Ihre Einwilligung verweigern?

Wenn Sie eine Frage mit „Ja“ beantworten, sollten Sie sich an Ihren Vorgesetzten oder den Datenschutzbeauftragten werden.

Wann muss ich betroffene Personen informieren?

Das Datenschutzrecht legt hohen Wert darauf, dass die Person, um deren Daten es geht, erkennen kann, welche Daten von ihr von welchem Unternehmen für welchen Zweck verarbeitet werden (§ 4 Abs. 3 BDSG). Die Person ist deshalb darüber zu unterrichten. Auch ein Hinweis auf Widerspruchsmöglichkeiten kann in Betracht kommen.

Allerdings entfällt in der Praxis die Pflicht zur Unterrichtung über den Umgang mit dem Daten oft bereits durch eine Ausnahmeregelung des Gesetzes. Die betroffene Person muss nämlich nicht informiert werden, wenn sie bereits Kenntnis von dem Umgang mit ihren Daten hat. So hat beispielsweise bei einem Kaufvertrag oder einem Liefervertrag der Betroffene bereits durch die Angabe seiner Daten bei der Bestellung eine Vorstellung von der Speicherung zu dem typischen Zweck.

Mitarbeiter, deren Daten vom Unternehmen gespeichert werden, haben auch das Recht, über den Umfang ihrer Daten Auskunft zu erhalten. Diese Auskunft sollte nur von einer zentralen Stelle des Unternehmens erteilt werden. Wenden Sie sich deshalb im Falle einer Auskunftsanfrage an Ihren Vorgesetzten und setzen Sie sich mit Ihrem betrieblichen Datenschutzbeauftragten in Verbindung.

Ihre Prüffrage

Hat der Betroffene hinreichende Information über:

- den Zweck der Verarbeitung seiner Daten,
- die dazu verwendeten Daten,
- den Namen und die Kontaktdaten Ihres Unternehmens,
- die Kategorien von Empfängern, an die die verarbeiteten Daten – falls das geplant ist – weitergegeben werden sollen,
- ein etwaiges Widerspruchsrecht?

Auch auf eine technisch sichere Datenverarbeitung ist stets zu achten

Der beste Datenschutz durch Unternehmen und Beschäftigte bringt wenig, wenn die Datensicherheit aus dem Blick gerät. Das Unternehmen wie der Beschäftigte müssen daher mit technischen und organisatorischen Vorkehrungen dafür Sorge tragen, dass personenbezogene Daten nicht abhandenkommen und nicht von Unbefugten eingesehen oder verändert werden. Bei einer zulässigen Übermittlung müssen die Daten sicher (nicht in einer offenen E-Mail) vom einen Unternehmen an das andere Unternehmen fließen. Schon durch kleine Unachtsamkeiten bei der Daten- und IT-Sicherheit können dem Unternehmen große Schäden entstehen, die nicht mehr rückgängig gemacht werden können.

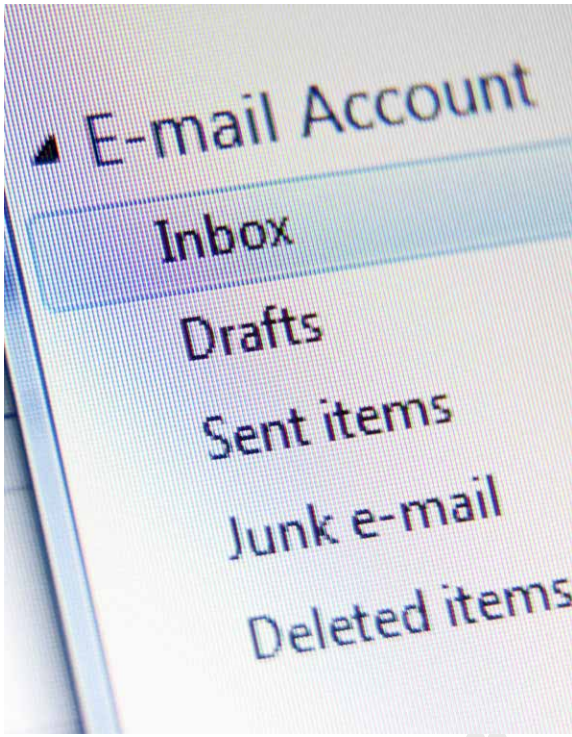
Es ist in Ihrem Arbeitsbereich Ihre Nebenpflicht, sowohl die Informationen über natürliche Personen als auch vertrauliche Firmeninformationen vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen. Um Pannen bei der Verwendung und Weitergabe personenbezogener Daten zu vermeiden, dürfen sie die Punkte auf den folgenden drei Seiten bitte niemals außer Acht lassen.

Beispiel für unzulässigen, unsicheren Datenumgang

Sie versenden eine geschäftliche E-Mail, achten beim Versenden aber nicht auf den korrekten Empfänger.

Bereits durch einen Klick können Daten so einen unberechtigten Dritten erreichen.

Denken Sie auch daran, dass E-Mails an Unternehmensfremde durch das allgemein zugängliche Internet versendet werden. Dritte können deshalb möglicherweise Einblick in die E-Mail-Inhalte nehmen, soweit sie nicht verschlüsselt sind.



Papierakten

Dokumente mit personenbezogenen Daten dürfen nicht in den normalen Müll, sondern müssen entweder mit einem Aktenvernichter vernichtet oder in vorgesehene Datenabfallbehälter gegeben werden. Achtung: Nicht jeder Aktenvernichter zerkleinert die Dokumente so klein, wie es das Datenschutzrecht verlangt. Die Standards zur Vernichtung von Datenträgern (DIN 66399) sind zu berücksichtigen.

Kommunikationsmaßahmen

Seien Sie grundsätzlich bei der Weitergabe von Daten vorsichtig. Achten Sie bei E-Mail-Kommunikation auf die richtige Eingabe der Adresse. Überprüfen Sie bei Faxübermittlung die eingegebene Nummer. Stellen Sie bei der Übermittlung von besonders wichtigen personenbezogenen Daten (Personaldaten, Gesundheitsdaten) eine persönliche Entgegennahme sicher oder verschlüsseln Sie das Dokument, wenn Sie es als Anhang einer E-Mail versenden. Versenden Sie geheimhaltungsbedürftige personenbezogene Daten im Zweifel nur verschlüsselt oder per Post.

Datentransport

Personenbezogene Daten sind nur auf firmeneigenen portablen Datenträgern (USB-Stick, Festplatte) und gegebenenfalls verschlüsselt zu transportieren. Fremde Datenträger dürfen nicht ungeprüft verwendet werden.

Datenverlust

Wenn Daten verloren werden, ist der Vorgesetzte zu informieren (siehe Abschnitt „Was mache ich, wenn doch einmal Daten abhandenkommen?“).

Schutz vor Mithören

Es ist dafür Sorge zu tragen, dass Unbefugte Ihre Telefongespräche nicht mitverfolgen können.

Sensibilität bei telefonischen Anfragen und Unternehmensfremden

Bei einer Auskunftsanfrage von Kunden oder Beschäftigten stellen Sie sich immer die Frage, ob der Anrufende berechtigt ist, die Information von Ihnen zu erhalten. Denn im Telefonat können Sie die Identität des Gegenübers nicht einfach feststellen. Überprüfen Sie also immer die Identität des Anrufers oder bieten Sie einen Rückruf Ihres Vorgesetzten an.

Fallen Ihnen unbekannte externe Personen in Ihrem Unternehmen auf, gehen Sie nicht einfach an ihnen vorbei, sondern fragen Sie ruhig nach deren Identität und Auftrag.

Verschlüsselung, Passwörter

Bei Passwörtern ist darauf zu achten, dass mindestens die Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) beachtet werden: Verwenden Sie eine Kombination aus Buchstaben, Zahlen und Sonderzeichen und wechseln Sie die Passwörter regelmäßig (Sie sollten diese Vorgaben auch für Ihre privaten Passwörter beachten).

Beim Verlassen des Rechners ist dieser zu sperren (bei Windows-Rechnern: WINDOWS-Taste + L, bei Mac-Rechnern: Control + Shift + Eject). Eine Reaktivierung darf nur über eine Passworteingabe möglich sein. Zusätzlich muss sich nach vorgegebener Zeit die automatische Bildschirmsperre einschalten, so dass in Pausenzeiten kein anderer an Ihren Rechner gehen kann.

Offene Augen und Ohren

Wenn Sie von unzulänglichen Datenverarbeitungen Kenntnis erhalten, informieren Sie Ihr Unternehmen darüber. Sie können dem Vorwurf einer „Einmischung“ in fremde Arbeitsbereiche aus dem Weg gehen, wenn Sie den betrieblichen Datenschutzbeauftragten ansprechen. Er ist auch gegenüber der Unternehmensleitung zur Verschwiegenheit bezüglich Ihres Namens verpflichtet. Sie brauchen also keine Befürchtung haben, dass er einen Vorfall mit Ihrem Namen weitergibt.

Ihre Prüffrage
Habe ich das in meiner Macht stehende getan, damit für die konkrete Sache nicht zuständige Kollegen oder außenstehende Dritte vom Inhalt meiner Datenverarbeitung keine Kenntnis erhalten?

Sie könnten folgenden Einwand haben
Mein Unternehmen hat erhebliche Mittel in die IT-Sicherheit gesteckt; sogar einen Informationssicherheitsbeauftragten haben wir. Weshalb muss ich auch mich zusätzlich um Passwortvorgaben, Schlüsselregelungen und sonstige Sicherheitsvorgaben im Unternehmen kümmern?

Die richtige Antwort
Die besten Unternehmensvorschriften nützen nichts, wenn sich die Beschäftigten nicht daran halten. Verstoßen die Beschäftigten gegen die Vorgaben, können sie ihrem Unternehmen erheblichen Schaden zufügen, weil die Sicherheit dann nicht mehr gewährleistet ist. Daher sind Arbeitsanweisungen verbindlich einzuhalten.

WAS IST BEI DER WEITERGABE VON DATEN AN ANDERE UNTERNEHMEN ZU BEACHTEN?

Ein Unternehmen arbeitet heute fast nie allein, sondern arbeitsteilig mit anderen zusammen. Es schaltet Zulieferer und sonstige Dienstleister ein, wie z. B. Schreibbüros, Aktenvernichtungsunternehmen, Rechenzentren, IT-Service-Dienstleister und Reinigungsfirmen. Dabei werden in verschiedenen Situationen personenbezogene Daten auch an solche Fremdfirmen zur weiteren Bearbeitung weitergegeben – aktiv durch Übersendung oder passiv durch Einräumen von Zugriffsrechten. Hier muss, kraft Gesetzes, in einem schriftlichen Vertrag sichergestellt werden, dass auch der Dienstleister und dessen Beschäftigte die gesetzlichen Datenschutzregelungen einhalten. Das den Auftrag gebende Unternehmen – also Ihr Unternehmen – bleibt nämlich auch für die ausgelagerte Datenverarbeitung rechtlich verantwortlich.

Die Fachleute nennen das Auftragsdatenverarbeitung. Daher sind auch die Datensicherheitsvorkehrungen bei anderen Unternehmen durch Ihr Unternehmen zu prüfen.

Wenn Sie für die Einschaltung von Fremdfirmen, zum Beispiel im Marketing, zuständig sind, haben Sie bei Auftragsvergabe die besonderen Anforderungen des Datenschutzes einzuhalten. Diese sind:

a) Abschluss eines schriftlichen Vertrages mit bestimmten, gesetzlich vorgegebenen Inhalten
b) Datensicherheitsbeschreibung
c) Kontrolle des Dienstleisters, beispielsweise durch Einsichtnahme in Prüfberichte
d) Dokumentation der Zuverlässigkeitseinschätzung.

Sie sind dabei in der Pflicht, Vorgaben der Geschäftsleitung oder des Vorgesetzten abzufragen. Auch der Datenschutzbeauftragte kann weiterhelfen.

Sind die datenschutzrechtlichen Voraussetzungen der Einschaltung einer Fremdfirma nicht erfüllt, ist die Verarbeitung durch die Fremdfirma datenschutzwidrig. Das eigene Unternehmen trägt dafür die Folgen.

Die Einschaltung von Dienstleistern, deren Arbeit einen eigenständigen Entscheidungsspielraum bedingt oder die aufgrund berufsrechtlicher Vorschriften nicht weisungsbefugt agieren dürfen, nennt man Funktionsübertragung. Hier muss eine Erlaubnisvorschrift für die Übermittlung an diese Dienstleister eingreifen (siehe Abschnitt „Wann darf mein Unternehmen Daten verarbeiten?“). Auch hier ist ein Vertrag erforderlich und es dürfen die personenbezogenen Daten durch den Dienstleister nur zweckgebunden verwendet werden. Ein Beispiel hierfür ist die Beauftragung eines Steuerberaters mit Aufgaben aus dem Steuerberatungsgesetz. Bei weiteren Fallkonstellationen kann der Datenschutzbeauftragte weiterhelfen.

DÜRFEN DATENBESTÄNDE ANGEREICHERT WERDEN?

Das Anreichern von Datenbeständen bedeutet, dass vorhandenen Informationen über Kollegen, Bewerber, Verbraucher, Kunden und Lieferantenbeschäftigte, Gäste oder andere natürliche Personen weitere Informationen zugefügt werden.

Beispiel

- Bei einer telefonischen Kundenbestellung auf Rechnung wird von einer Kreditauskunftei eine Information über die Zahlungsfähigkeit des Betroffenen abgefordert und dem Kundendatensatz hinzugespeichert.
- Bei einem Bewerber wird ein berufliches soziales Netzwerk wie Xing oder LinkedIn zu Rate gezogen, um weitere Informationen über den Bewerber zur Bewerberauswahl zu erhalten.

Solche Anreicherungen müssen – ebenso wie jeder andere Datenumgang – datenschutzrechtlich erlaubt sein (siehe Abschnitt „Warum betreibt mein Unternehmen Datenschutz?“ und Abschnitt „Was ist bei der Weitergabe von Daten an andere Unternehmen zu beachten?“). Nur wenn es objektiv erforderlich und verhältnismäßig ist und damit ein gesetzlicher Erlaubnistatbestand gegeben ist, darf eine solche Anreicherung erfolgen. Bei Bewerbungen zum Beispiel ist es nicht erlaubt, Daten aus rein privaten sozialen Netzwerken zu erheben und mit den Bewerbungsdaten zu speichern.

WIE VERHALTE ICH MICH, WENN DOCH EINMAL DATEN ABHANDENKOMMEN?

Kein Unternehmen ist 100%ig sicher. Es kann in jedem Unternehmen irgendwann einmal einen „Datensicherheitsvorfall“ geben. Das Wichtigste ist es dann, etwaigen Schaden von den betroffenen Personen (deren Informationen abhandengekommen sind) und vom Unternehmen abzuwenden. Für bestimmte Datenarten hat der Gesetzgeber für den Fall des Abhandenkommens besonders strenge Anforderungen an die Unternehmen gestellt. Sie reichen bis zur Information der zuständigen Datenschutzaufsichtsbehörde. Der Mechanismus, den das Gesetz vorsieht (Information von Aufsichtsbehörde und Betroffenen), setzt an erster Stelle Ihren Einsatz als Beschäftigter voraus. Einen Datenverlust, den Sie feststellen, müssen Sie sofort den zuständigen Stellen des Unternehmens melden. Das Unternehmen muss dann die zuständige Aufsichtsbehörde in Kenntnis setzen.

Datenarten, die Anzeigepflichten auslösen können (§ 42a BDSG)

a) Daten zu Bank- oder Kreditkartenkonten.
b) sensible Daten (zur Gesundheit, zu politischen Meinungen, zu religiösen oder philosophischen Überzeugungen, über die rassische und ethnische Herkunft, über die Gewerkschaftszugehörigkeit oder über das Sexualleben).
c) Daten über begangene oder vermutete Straftaten oder Ordnungswidrigkeiten.
d) Personenbezogene Daten, die einem Berufsgeheimnis unterliegen.
e) Bei Webservern auch Bestands- oder Nutzungsdaten (§ 15a TMG).

Ihre Vorgehensweise
Wenn Ihnen oder Kollegen ein Laptop, ein Tabletcomputer, ein Smartphone, ein Speicherstick, Memos, Akten mit Informationen über Beschäftigte, Bewerbern, Kunden, Interessenten, Gästen, Veranstaltungsteilnehmer und/oder Pressevertreter abhandenkommen, handeln Sie schnell: Informieren Sie Ihre Vorgesetzten, den betrieblichen Datenschutzbeauftragten und die Geschäftsleitung per E-mail oder per Hauspost, notfalls mündlich.

Möglicherweise gibt es auch eine Betriebsvereinbarung, die regelt, wie Sie sich verhalten und wen Sie informieren müssen.

WANN MÜSSEN DATEN ÜBER PERSONEN GELÖSCHT WERDEN?

Ihr Unternehmen muss sich darum kümmern, was in der Zukunft mit abgeschlossenen Vorgängen passiert, die personenbezogene Daten enthalten. Es hat datenschutzrechtlich sicherzustellen, dass nach Zweckerreichung bzw. nach Ablauf der gesetzlichen Fristen der Zugriff auf Bewerber-, Mitarbeiter-, Kunden-, Ansprechpartner-, Gäste- und Teilnehmerdaten verhindert wird. Im Idealfall besteht im Unternehmen ein Aufbewahrungskonzept für die verschiedenen vorhandenen Datenarten und einer jeweils festgelegten Löschungsfrist. Zu berücksichtigen sind dabei auch Zwischenspeicherungen, wie in E-Mails oder auf Webservern, und Ausdrucke für die Fachabteilungen.

Grundsätzlich sind personenbezogene Daten zu löschen, wenn sie nicht mehr gebraucht werden. Konkrete Fristen nennt das Gesetz hierzu nicht, sondern hält Daten für löschenswert, „sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist“ (§ 35 Abs. 2 Satz 1 Nr. 3 BDSG). Es ist daher entscheidend, ab wann das Unternehmen die Daten nicht mehr konkret benötigt.

Ausnahmsweise bestehen gesetzliche Aufbewahrungspflichten, z. B. bei Rechnungsunterlagen. Dann brauchen die betroffenen Daten nicht gelöscht werden, obwohl sie das Unternehmen nicht mehr unmittelbar braucht. Der gesetzliche Zweck (Betriebsprüfung) verbietet die Löschung dann sogar und zwingt zur Aufbewahrung. Das Unternehmen ist allerdings zum sogenannten Sperren der Daten verpflichtet: Die Daten müssen derart „weggeschlossen“ werden, das der Zugriff der Mitarbeiter für andere Zwecke ausgeschlossen ist.

Viele Daten stellen wertvolle immaterielle Güter für Unternehmen dar. Als Beschäftigter sind Sie nicht befugt, von sich aus oder unter pauschalem Verweis auf Datenschutzgesetze, personenbezogene Daten im Unternehmen einfach zu löschen. Es ist Sache des Unternehmens, durch technische Einrichtungen Daten nach Ablauf bestimmter Fristen automatisch sperren und löschen zu lassen oder den Beschäftigten mit einer konkreten Arbeitsanweisung aufzugeben, bestimmte Datenbestände zu löschen.

WER KONTROLLIERT DEN DATENSCHUTZ?

Die Unternehmensleitung

Die Unternehmensleitung handelt datenschutzkonform, wenn sie ihre Beschäftigten dazu verpflichtet, bei ihrer jeweiligen Tätigkeit für das Unternehmen datenschutzkonform zu handeln (Datenschutzarbeitsanweisung). Diese Datenschutzarbeitsanweisungen werden typischerweise von verschiedenen Stellen im Unternehmen aufgestellt und umgesetzt. An erster Stelle steht die Verpflichtungserklärung zur Verschwiegenheit (siehe Abschnitt „Weshalb bin ich als Beschäftigter für den Datenschutz meines Unternehmens mitverantwortlich?“, dort unter „Pflichten des Beschäftigten“). Sie wird häufig bei der Einstellung gegenüber der Personalabteilung abzuzeichnen sein (Muster siehe Abschnitt „Anlage Beschäftigtenverpflichtungserklärung zur Verschwiegenheit“). Der Beschäftigte erhält eine Kopie dieser von ihm unterzeichneten Erklärung und zugleich wichtige Vorschriften zum Datenschutz (siehe Abschnitt „Anlage Wichtige ausgewählte Datenschutzvorschriften“) sowie ein Datenschutzmerkblatt (wie z. B. diese Broschüre) ausgehändigt.

Der betriebliche Datenschutzbeauftragte

Innerhalb des Unternehmens überprüft der betriebliche Datenschutzbeauftragte im Rahmen seiner Tätigkeit, ob die in Frage stehenden personenbezogenen Daten vom Unternehmen und von Ihnen zulässig erhoben werden, für den jeweiligen Verarbeitungszweck erforderlich sind, zweckgebunden eingesetzt und unter angemessenen Sicherheitsvorkehrungen verarbeitet werden. Dabei berät er die Geschäftsleitung und die Beschäftigten und steht bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten zur Verfügung. Die Aufgabe, den Datenschutz sicherzustellen, hat er dagegen nicht. Diese Aufgabe liegt bei der Unternehmensleitung und Ihnen.

Sofern Sie sich an den betrieblichen Datenschutzbeauftragten wenden, ist er der Geschäftsleitung gegenüber zur Verschwiegenheit über Ihren Namen verpflichtet. Sollten Sie Fragen zum Datenschutz haben, können Sie sich also nicht nur an Ihren Vorgesetzten wenden, sondern auch gewissenhaft den betrieblichen Datenschutzbeauftragten ansprechen.

Die Datenschutzaufsichtsbehörden

Die Landesbeauftragten für den Datenschutz (in Bayern: Landesamt für Datenschutzaufsicht) kontrollieren als staatliche Aufsichtsbehörden die Einhaltung des Datenschutzes. Zuständig ist in der Regel die Aufsicht in dem Bundesland, in dem das Unternehmen seinen (Haupt-)Sitz hat. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist im Bereich der Wirtschaft nur für die Telekommunikations- und Postdienstunternehmen zuständig.

WAS MACHE ICH, WENN MEIN UNTERNEHMEN DATEN IN LÄNDER AUSSERHALB DER EUROPÄISCHEN UNION SENDET?

Wenn Ihr Unternehmen Geschäfte in Staaten innerhalb des Europäischen Wirtschaftsraums (EU, Island, Norwegen, Liechtenstein) macht und dabei personenbezogene Daten fließen, ergeben sich keine Besonderheiten (siehe Abschnitt „Warum betreibt mein Unternehmen Datenschutz?“ und Abschnitt „Was ist bei der Weitergabe von Daten an andere Unternehmen zu beachten?“).

Wenn dagegen ein Datenfluss in Staaten außerhalb des Europäischen Wirtschaftsraums erfolgen soll, schafft das Datenschutzrecht zusätzliche Anforderungen. Der Transfer der personenbezogenen Daten in solche Drittländer muss besonders gerechtfertigt sein. Fragen Sie im Zweifel Ihren Vorgesetzten nach konkreten Arbeitsanweisungen. Bereits ein internationaler Datenschutzvertrag kann diese Rechtfertigung darstellen. Doch es ist in der Regel Sache der Rechtsabteilung oder des Rechtsanwalts Ihres Unternehmens, die notwendigen Verträge aufzustellen. Der Datenschutzbeauftragte hat hierauf hinzuweisen, zu beraten und die Umsetzung zu kontrollieren.

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

WO FINDE ICH MEHR INFORMATIONEN?

„Bundesdatenschutzgesetz: Text und Erläuterungen”. Hrsg.: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI-Info Nr. 1).

ANLAGE

Beschäftigtenverpflichtungserklärung zur Verschwiegenheit

Unternehmen (Firma): _____

Verpflichtungserklärung gem. § 5 BDSG:
Geschäfts-/Betriebsgeheimnisse
und Datengeheimnis (Datenumgang)

_____ _____
vollständiger Name Geburtsdatum

_____
Anschrift

Ich bin beschäftigt:

☐ direkt im oben angegebenen Unternehmen (Angestelltenstatus)
☐ als freier Mitarbeiter/Freelancer
☐ in einem vom oben angegebenen Unternehmen beauftragten anderen Unternehmen

und erlange im Rahmen meiner Tätigkeit Kenntnis von personenbezogenen Daten sowie Daten betreffend mein (oben angegebenes) Unternehmen und/oder betreffend mit diesem verbundene Unternehmen und Geschäftspartner und erkläre das Folgende:

Über die Sorgfalts- und Geheimhaltungspflichten im Zusammenhang mit der Bearbeitung von Projekten, personenbezogenen Daten und Unternehmensdaten und im Umgang mit Informationstechnik bin ich unterrichtet worden.

Personendaten: Mir ist es insbesondere untersagt, personenbezogene Daten – dies sind z.B. Informationen über Kunden, Interessenten, Vorgesetzte, Kollegen, Ansprechpartner – zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck

zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen. Das Bundesdatenschutzgesetz schützt alle Daten natürlicher Personen, die in Dateiform (d.h. geordnet) oder auch in Personalakten aufgezeichnet oder verarbeitet werden. Hierzu zählen nicht nur Aufzeichnungen auf maschinell lesbaren Datenträgern, sondern auch Angaben auf Formularen, Karteikarten, Mikrofilmen u.ä., soweit sie nach mehreren Merkmalen sortiert werden können. Informationen über meine Kolleginnen und Kollegen sind darüber hinaus in jedem Fall geschützt und nur für die Betriebszwecke zu verwenden. Das gilt natürlich nicht, wenn ich mich außerhalb des Betriebsverhältnisses zu privaten Zwecken mit meinen Kolleginnen und Kollegen austausche. Die Verpflichtung besteht – soweit zulässig – auch nach der Beendigung meiner Tätigkeit fort.

Geschäfts- und Betriebsgeheimnisse: Die Geheimhaltungspflicht gilt auch für technische, kaufmännische und sonstige geheimhaltungsbedürftige Informationen im Unternehmen, für verbundenen Unternehmen und Geschäftspartner wie beispielsweise interne Kunden- und Preislisten. Dazu gehören auch Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung ein berechtigtes Interesse besteht.

Verstöße gegen meine Obliegenheiten, insbesondere die innerbetriebliche Geheimhaltungspflicht, können zivilrechtlich Schadensersatzpflichten begründen, strafrechtlich geahndet (§§ 203, 204 Strafgesetzbuch, §§ 17-19 Gesetz gegen den unlauteren Wettbewerb) und Verstöße gegen das Datengeheimnis nach §§ 43, 44 BDSG verfolgt werden. Der unbefugte Abruf geschützter Daten und die Zerstörung von Daten ist ebenfalls strafbar (§§ 202a, 303a StGB).

Mir sind

☐ **wichtige ausgewählte Datenschutzvorschriften** sowie
☐ die Broschüre **„Was muss ich als Beschäftigter vom Datenschutz unbedingt wissen?“**

ausgehändigt worden. Ich erkläre, diese Informationen zur Kenntnis genommen zu haben, sie zu beachten und mich vor allem auch an meine Verschwiegenheitspflichten zu halten.

_____ _____
Ort, Datum Unterschrift des Beschäftigten

Gesetzesauszug zur Verpflichtungserklärung

(siehe auch Anlage „Die wichtigen Rechtsvorschriften im Wortlaut“)

§ 5 BDSG [Datengeheimnis]

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 BDSG [Bußgeldvorschriften] - Auszug -

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

…

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

…

§ 44 BDSG [Strafvorschriften]

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

ANLAGE

Die wichtigsten Begriffe

Anonymisieren

Daten so behandeln, dass sie endgültig nicht mehr auf eine bestimmte oder bestimmbare Person hinweisen.

Aufsichtsbehörden

Die Einhaltung der Vorschriften zum Datenschutz wird in Deutschland durch besondere Aufsichtsbehörden kontrolliert. Dies sind die Landesbeauftragten und die Bundesbeauftragte für den Datenschutz. Für Unternehmen und Länderbehörden sind die Landesbeauftragten zuständig. Speziell für Post- und Telekommunikationsunternehmen und für alle Bundesbehörden ist die Bundesbeauftragte die richtige Ansprechpartnerin. Personen, die Datenmissbrauch befürchten, können sich an die jeweilige Behörde in ihrem Bundesland wenden. Auch Unternehmen oder andere Behörden können sich dort zum Datenschutz beraten lassen. Die Aufsichtsbehörden veröffentlichen jährliche Tätigkeitsberichte, u.a. zu Datenschutzvorfällen in ihrem Bundesland.

Auftragsdatenverarbeitung

Wenn personenbezogene Daten von anderen Unternehmen zur Erfüllung der Aufgaben des eigenen Unternehmens verarbeitet werden, spricht man von „Auftragsdatenverarbeitung“. Dabei bleibt das Unternehmen, das den Auftrag für die Datenverarbeitung gegeben hat, für die Einhaltung der Datenschutzvorschriften beim externen Dienstleister verantwortlich. Die Verträge müssen entsprechend gestaltet werden.

Auskunftsanspruch

Jede Person hat in Deutschland ein Recht zu erfahren, welche sie betreffenden Daten für welche Zwecke gespeichert oder weitergegeben werden. Denn nur wer weiß, was über ihn gespeichert und verarbeitet wird, kann die Einhaltung der Datenschutzvorschriften beim Umgang mit seinen Daten bewerten.

Beschäftigte

Sowohl Personen, die in einem Unternehmen angestellt sind (Arbeitnehmer), als auch arbeitnehmerähnliche Personen, Auszubildende, Bewerber, gekündigte Arbeitnehmer, Praktikanten und Leiharbeitnehmer.

Datenanreicherung

Jedes Unternehmen verfügt über personenbezogene Daten von Beschäftigten, Kunden, Lieferanten usw. Es ist grundsätzlich möglich, aus anderen Quellen weitere Daten zu erfassen und die Datensätze zu ergänzen. So kann beispielsweise ein Unternehmen seinen Kundenadressdatensatz um die aktuelle Adresse aus dem Melderegister „anreichern“.

Datenschutzabmahnung

Abmahnung wegen Verstoßes gegen die Datenschutzvorschriften. Sie wird – anders als eine Ermahnung – mit der Konsequenz erklärt, dass der Arbeitnehmer im Wiederholungsfall mit der Kündigung rechnen muss.

Datenschutzbeauftragter/ betrieblicher Beauftragter
Die unabhängige Stelle des Unternehmens, die sich um den Einhaltung der Datenschutzvorschriften kümmert. Dazu erfasst der betriebliche Datenschutzbeauftragte alle Prozesse, die personenbezogene Daten nutzen. Zudem kontrolliert der Beauftragte, ob in den einzelnen Prozessen datenschutzkonform gearbeitet wird. Schließlich schult er die Beschäftigten in Bezug auf Datenschutzvorschriften. Er ist verpflichtet, alle Anfragen und Hinweise vertraulich zu behandeln, auch gegenüber der Geschäftsleitung.

Datenschutzpflichten
Die Vorschriften des Datenschutzrechts gelten für das Unternehmen und auch seine Beschäftigten. Wer auf personenbezogene Daten im Unternehmen zugreifen kann, der muss wissen, wie diese Daten genutzt werden dürfen – und was nicht zulässig ist.

Datenverlust
Ein Verlust von personenbezogenen Daten durch Unternehmen kann für die Betroffenen unangenehm sein. Daher müssen hinreichende Datensicherheitsmaßnahmen eingerichtet sein, um Datenverluste zu verhindern. Beschäftigte sind verpflichtet, dem Arbeitgeber jeden Datenverlust zu melden.

Datenschutzverstoß
Eine Verletzung von Datenschutzvorschriften, die Sanktionen auslösen kann.

Datenschutzvorschriften
Alle staatlichen Vorschriften, die den Umgang mit personenbezogenen Daten regeln, beispielsweise das Bundesdatenschutzgesetz, das Sozialgesetzbuch, das Telemediengesetz und auch das Strafgesetzbuch (siehe Anlage Datenschutzvorschriften).

Datensicherheit (IT-Sicherheit)
Alle Maßnahmen, um im Unternehmen vorhandene Daten sicher zu verwahren und gegen Angreifer von außen (Hacker, Kriminelle, Spione) zu schützen.

Direktmarketing
Werbemaßnahmen, die sich direkt an einen einzelnen Kunden oder bestimmte Interessenten richten, z.B. Werbe-E-Mails, Werbeanrufe oder Werbebriefe. Hier werden jeweils personenbezogene Daten genutzt.

Einwilligung
Die Verarbeitung personenbezogener Daten ist immer zulässig, wenn die betroffene Person ihr Einverständnis informiert und dokumentiert erklärt hat. So kann beispielsweise ein Unternehmen seine Kunden online oder per Post bitten, in die künftige Verwendung der Daten für Werbung einzuwilligen. Eine Einwilligung ist immer nur wirksam, wenn sie freiwillig, d.h. auch ohne unterschwelligen/psychischen Zwang abgegeben wird.

Erlaubnisvorschrift/gesetzliche Erlaubnis
Das Datenschutzrecht ist ein sogenanntes „Verbotsgesetz". Das bedeutet: Jeder Umgang mit personenbezogenen Daten ist zunächst untersagt. Nur wenn eine gesetzliche Vorschrift oder die Einwilligung der betroffenen Person es erlaubt, kann mit den Daten umgegangen werden.

Ermahnung
Mündliche oder schriftliche Erklärung des Arbeitgebers gegenüber dem Beschäftigten, dass dieser gegen seine (Datenschutz-)Pflichten verstoßen hat. Sie hat – anders als eine Abmahnung – keine rechtlichen Konsequenzen und ist die schwächste Stufe einer Rüge des Verhaltens des Beschäftigten.

Informationelle Selbstbestimmung
Jeder Mensch hat einen verfassungsrechtlichen Anspruch auf Schutz seiner persönlichen Informationen. Man soll grundsätzlich selbst bestimmen können, was andere über einen wissen.

Nicht nur Ärzte oder Rechtsanwälte müssen die Angaben ihrer Patienten/Mandanten geheim halten. Auch für normale Unternehmen gilt, dass sie die Privatsphäre ihrer Beschäftigten, Kunden und Lieferanten wahren müssen. Da aber auch Unternehmen berechtigte Interessen haben, mit personenbezogenen Daten umzugehen, schaffen Datenschutzgesetze und Betriebsvereinbarungen einen Ausgleich zwischen informationellem Selbstbestimmungsrecht und Verwendungsinteressen.

Pseudonymisierung
Methode, um eine Identifizierung einer Person auszuschließen oder wenigstens zu erschweren. Die pseudonyme Nutzung ist ein besonders datenschutzfreundlicher Umgang mit personenbezogenen Daten. Dazu können z.B. Personalnummern statt der Namen verwendet werden, etwa im Rahmen einer Revision.

Schulung
Das Gesetz schreibt vor, dass die Beschäftigten über Datenschutz und ihre Pflichten informiert sein müssen. Dafür zu sorgen, ist Sache des Unternehmens. Meist bietet die betriebliche Datenschutzbeauftragte entsprechende Informations- und Schulungsveranstaltungen an.

Sensible Daten/Sensitive Daten
Bei Gesundheitsdaten und Angaben über ethnische Herkunft, politische Meinung, religiöse oder philosophische Ausrichtung, Gewerkschaftszugehörigkeit oder das Sexualleben gilt ein besonders strenger Maßstab für den Datenumgang.

Tätigkeitsberichte
In erster Linie ein öffentlicher Arbeitsbericht der Aufsichtsbehörde für den Datenschutz. Auch der Datenschutzbeauftragte in Unternehmen und Behörden kann solche Berichte erstellen. Sie sind jedoch nur für die Leitungsorgane bestimmt.

Verfahrensverzeichnis
Eine umfassende Auflistung in einer elektronischen Datei oder Papierakte, in der notiert ist, an welchen Stellen im Unternehmen Daten verarbeitet werden und wie die Verarbeitung erfolgt. Anhand dieses Verzeichnisses kann die Einhaltung der Datenschutzvorschriften kontrolliert werden.

Verpflichtungserklärung/Verpflichtung auf das Datengeheimnis
Alle Beschäftigten, die personenbezogene Daten verarbeiten, müssen sich dem Unternehmen gegenüber verpflichten, die Datenschutzvorschriften einzuhalten und eine entsprechende Erklärung unterschreiben.

Zweckbindung
Im Allgemeinen dürfen personenbezogene Daten allein zu dem Zweck genutzt werden, zu dem sie gesammelt/gespeichert wurden. Ausnahmsweise darf ein Unternehmen Daten aus einem Kundengeschäft nicht nur für die Vertragsabwicklung nutzen, sondern auch dafür Kunden auf weitere Produkte und Dienstleistungen aufmerksam zu machen (siehe Direktwerbemaßnahmen).

Weitere Begriffe und Vorschriften finden Sie erklärt im Internetauftritt der Bundesbeauftragten:
www.bfdi.bund.de/bfdi_wiki

ANLAGE
Die wichtigen Rechtsvorschriften im Wortlaut

§ 22 Kunsturhebergesetz
Recht am eigenen Bild
Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

§ 201a Strafgesetzbuch
Verbot des Ausspähens
Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.

§ 202a Strafgesetzbuch
Verbot des Zugriffs auf fremde Daten
Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 203 Strafgesetzbuch
Verbot, Geheimnisse an Kollegen weiterzugeben
Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als (…) Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, (…) Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Amtsträger, für den öffentlichen Dienst besonders Verpflichteten, Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt, (…) anvertraut worden oder sonst bekanntgeworden ist.

§ 303a Strafgesetzbuch
Verbot, personenbezogene Daten zu unterdrücken
Wer rechtswidrig Daten (…) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 4 Bundesdatenschutzgesetz

Erlaubnis zum Umgang mit personenbezogenen Daten

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

§ 4a Bundesdatenschutzgesetz

Anforderungen an eine Einwilligung

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

§ 5 Bundesdatenschutzgesetz

Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 17 Gesetz gegen unlauteren Wettbewerb

Verbot des Verrat von Geschäfts- und Betriebsgeheimnissen

Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 9 Bundesdatenschutzgesetz

Pflicht zur Gewährleistung von Datensicherheit

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 91 Aktiengesetz

Pflichten des Vorstandes

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

§ 11 Bundesdatenschutzgesetz

Verantwortlichkeit des Auftraggebers bei Beauftragung anderer Unternehmen

Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. (…) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen (…). Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

§ 13 Bundesdatenschutzgesetz

zulässiger Datenumgang bei Behörden

Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

§ 28 Bundesdatenschutzgesetz

zulässiger Datenumgang bei Unternehmen

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, (…) wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist, (…) soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder (…) wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. (…) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine

Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist (…). Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig.

§ 32 Bundesdatenschutzgesetz

zulässiger Umgang mit Beschäftigtendaten

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunk-te den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

§ 5 Telemediengesetz

zulässiger Umgang mit Internetdaten

Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

§ 43 Bundesdatenschutzgesetz

Bußgelder bei Datenschutzverletzungen

Die Ordnungswidrigkeit kann (…) mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen.

§ 44 Bundesdatenschutzgesetz

Strafen bei Datenschutzverletzungen

Wer eine (…) Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit einer Geldstrafe bestraft.

§ 88 Telekommunikationsgesetz

Fernmeldegeheimnis

Den (…) Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

§ 100 Telekommunikationsgesetz

Erlaubnis zur Datenverwendung durch TK-Dienstleister

Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. (…) Soweit erforderlich, darf der Diensteanbieter bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte die Bestandsdaten und Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind.

Die STIFTUNG DATENSCHUTZ wurde 2013 von der Bundesrepublik Deutschland gegründet. Als unabhängiger Akteur stellt die gemeinnützige Bundesstiftung ein Bindeglied zwischen Gesellschaft, Wirtschaft, Forschung und Politik dar. Als neutrale Plattform zur Förderung des Selbstdatenschutzes ergänzt sie bestehende Initiativen und die Datenschutzaufsichtsbehörden.

Ein Ziel der Stiftungsarbeit ist es, die Sensibilität für den Wert von Privatheit und persönlichen Informationen zu steigern. Mehr Wissen über die Möglichkeiten eines bewussten Umgangs mit eigenen Daten soll den Menschen bei der Wahrung ihrer Persönlichkeitsrechte helfen. Neben der Aufklärungsarbeit wird die Stiftung nach neuen effektiven Wegen zum Schutz der Privatsphäre suchen und Handlungsempfehlungen entwickeln.

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
Karl-Rothe-Straße 10–14
04105 Leipzig
Telefon 0341/5861 555-0
Telefax 0341/5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org