5.5. DATENSCHUTZHANDBUCH

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 Geschäftsleitung, die Rechtsabteilung und der oder die betriebliche Datenschutzbeauftragte befassen, doch trifft in der heutigen Arbeitswelt nahezu jeder Beschäftigte auch eigene Entscheidungen zur Datenverarbeitung.

Mitteilung der Geschäftsleitung

Als Unternehmensleitung sind wir verpflichtet, unsere Belegschaft zum Datenschutz aufzuklären. Das bedeutet, dass unsere Mitarbeiterinnen und Mitarbeiter wissen, dass sie personenbezogene Daten nur nach unserer Weisung verarbeiten dürfen. Wir nutzen deshalb diesen Leitfaden um die Beschäftigten zu sensibilisieren und über die grundlegenden Anforderungen aufzuklären.

Dieser Leitfaden kann konkrete Arbeitsanweisungen zum Umgang mit bestimmten Datenarten jedoch nicht ersetzen und wird daher ggf. durch weitere Anweisungen ergänzt.

Dieser Leitfaden liefert jedoch die gesetzlich vorgesehenen Grundinformationen und allgemeine datenschutzbezogene Arbeitsanweisungen.

Bitte Lesen Sie diesen Leitfaden aufmerksam durch.

Freundliche Grüße,

Franz Wieser
Geschäftsführer Karl Wieser OHG

Geheimnisse im Unternehmen

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;

Die Unternehmensleitung sorgt bereits dafür, dass diese Geheimhaltung vertraglich vereinbart wird – nicht nur mit Mitarbeitern in Arbeitsverträgen, sondern auch mit externen Dienstleistern wie Zeitarbeitsfirmen, Lieferanten und Steuerberatern in den Dienstleistungsverträgen. So verpflichten sich die Vertragspartner, Betriebs- und Geschäftsgeheimnisse zu wahren.

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 Datenschutzgrundverordnung und durch das ergänzende italienische Anpassungsgesetz. Das Ziel des Datenschutzes besteht untern anderen 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 und bedeuten, dass schon dann ein Datenschutzverstoß vorliegt, wenn personenbezogene Daten angesehen werden, die für die Arbeitsaufgaben nicht benötigt werden, Informationen über Kunden weitergeleitet werden, ohne dass es dafür eine gesetzliche Erlaubnis gibt.

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.

Unmittelbar zuzuordnen ist der Person z.B. ihr Name, ihre Funktion, wenn es zum Beispiel nur eine IT-Leiterin im Unternehmen gibt.

Mittelbar kann sogar eine IP-Adresse einer bestimmten Person zugeordnet werden. Dieses Beispiel zeigt, dass vor allem beim mittelbaren Personenbezug der Zusammenhang betrachtet werden muss, wenn es darum geht zu entscheiden, ob es sich um personenbezogene Daten handelt.

Darüber hinaus gibt es **besondere Kategorien von personenbezogene Daten**, die noch strenger

geschützt sind: Das sind Daten, aus denen eine ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben
oder der geschlechtlichen Orientierung einer natürlichen Person.

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 solchen Daten immer besonders fachkundiger Rat eingeholt werden.

Verstöße

Bei der Verarbeitung personenbezogener Daten müssen umfangreiche Datenschutzvorschriften beachtet werden, denn Verstöße – nicht nur bei Vorsatz, sondern auch aus fahrlässiger Unwissenheit oder Nachlässigkeit – können dem Unternehmen und auch dem handelnden Mitarbeiter nachteilige Folgen bereiten.

In erster Linie geht es natürlich darum, Nachteile aus rechtswidriger oder datenunsicherer Verarbeitung von den Betroffenen fernzuhalten.

Der vorliegende Leitfaden 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. Auch 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 Datenschutzverstöße

Ein Angestellter der Personalabteilung will einen Vorgesetzten über die Arbeitsunfähigkeit einer Mitarbeiterin per unverschlüsselter E-Mailinformieren. Bei der Adresseingabe vertippt er sich und schickt die Mail mit den sensiblen gesundheitsbezogenen Daten versehentlich an einen 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 die Idee, 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...), über datenschutzgerechtes
Verhalten belehrt und auf das Datengeheimnis verpflichtet werden.

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
Beschäftigten Sanktionen und andere nachteilige Folgen.

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

Das Datenschutzrecht will jeden Menschen davor schützen, dass ihm durch den Umgang mit seinen persönlichen Daten Schaden zugefügt wird.

Um diesen Zweck zu erreichen, sieht das Datenschutzrecht Strafen für Unternehmen und auch Mitarbeiter vor. Da Datenschutz in der Öffentlichkeit eine so große Rolle spielt, vermeiden datenschutzkonform handelnde Unternehmen zudem negative Presse über sich.

Rechtliche Grundlagen

Die wichtigsten Regelungen für den Datenschutz sind die neue Europäische Datenschutz-Grundverordnung (DSGVO) und das ergänzende neue italienische Anpassungsgesetz. Die DSGVO gilt von Mai 2018 an unmittelbar in allen EU-Mitgliedsstaaten. Diese können sich ergänzende eigene Regelungen geben.

Das Datenschutzrecht schützt personenbezogene Daten in jeder Form, nicht nur auf Computern oder in Datenbanken, sondern auch auf Papier.

Jede Verarbeitung personenbezogener Daten ist zunächst verboten, solange sie nicht ausnahmsweise erlaubt ist. Diese Erlaubnis kann auf ganz unterschiedliche Weise zustandekommen (Art. 6 DSGVO) und zwar:

- bei einer Einwilligung der betroffenen Person
- 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 zum Einsatz.

Anforderungen an die Einwilligung

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.

Wer sorgt für guten Datenschutz?

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.

Dieser Leitfaden enthält allgemeinere Vorgaben als die datenschutzbezogenen Arbeitsanweisungen und ermöglicht es den Beschäftigten, sich im konkreteren Anwendungsfall für datenschutzkonformes Handeln zu entscheiden.

Falls Sie bei der Bewertung unsicher sind, müssen Sie sich an Ihren Vorgesetzten wenden.

Manchmal liegt es auf der Hand, manchmal ist es unklar, ob die eigene Datenverarbeitung datenschutzrechtlich zulässig ist. Hier kann Ihnen diese Regel helfen:

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.

Der Datenschutzbeauftragte berät und prüft

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 Datenschutzfolgenabschätzung 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 und verantwortet die Zuweisung von Zuständigkeiten, die 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 (Garante per la protezione die dati personali)

Für jedes Unternehmen gibt es eine zuständige Behörde, die den Datenschutz im Unternehmen überwachen soll und vor allem auf Anzeigen und Beschwerden von Betroffenen reagiert. Für die
meisten Unternehmen ist diese Behörde der *Garante per la protezione die dati personali*

Der Bußgeldrahmen ist mit der Datenschutzgrundverordnung erheblich erhöht worden. Unternehmen sind nun bei schwersten Datenschutzverstößen von einem Maximalbußgeld von bis zu 20 Mio. EUR oder bis zu vier Prozent ihres weltweiten Jahresumsatzes bedroht.

Hinweise für die Praxis

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:

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

1) Erlaubnisprüfung

Ohne eines der gesetzlichen Erlaubnisse (Einwilligung, Rechtsvorschrift, Betriebsvereinbarung, Vertrag oder dessen Vorbereitung auf Initiative des Kunden, objektiv überwiegendes Interesse des Unternehmens) darf das Unternehmen keine personen-
bezogenen Daten verarbeiten. Entscheidend ist dabei immer, ob die Kundendaten auch tatsächlich erforderlich sind, um den konkreten Zweck zu erreichen: Für den Brötchenkauf beim Bäcker 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 von Daten zur fahrenden Person notwendig.

Beispiele:

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 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: Interesse des Unternehmens im Rahmen der Interessenabwägung).

2) Information

Das Datenschutzrecht verlangt nicht nur, dass die Datenverarbeitung zulässig ist – die betroffene Person muss auch darüber 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 dies geschieht und um welche Daten es sich handelt (Art. 12-14 DSGVO). Auch ein Hinweis auf ein Widerspruchsrecht ist ein Muss.

3) Datensichere Verarbeitung

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.

Beispiele: 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 Verschlüsselung versendet werden. Dritte können möglicherweise Einblick in die E-Mail-Inhalte nehmen, wenn sie nicht verschlüsselt sind.

Es ist daher Ihre Pflicht, 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 über natürliche Personen. Ein Zuviel an personenbezogenen Daten ist rechtswidrig. Das ist auch deshalb wichtig, weil die betroffenen Personen Auskunft über ihre im Unternehmen gespeicherten Daten verlangen können. Das Unternehmen ist dann verpflichtet, alle über die betroffene Person gespeicherten Daten offen zu legen.

Papierakten

Dokumente mit personenbezogenen Daten dürfen nicht in den normalen Müll oder den 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 Vorgesetzte umgehend zu informieren.
Passwörter

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 die Sperrung nach vorgegebener Zeit automatisch aktiviert werden, damit kein Unbefugter den Computer benutzen kann, wenn Sie das Sperren einmal versäumt haben.

Schutz vor Mithören

Führen Sie Telefonate mit sensiblen Inhalten so, dass Unbefugte das Gespräch nicht mitverfolgen 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 von unzulänglichen Datenverarbeitungen Kenntnis erhalten, informieren Sie das Unternehmen darüber. Sie können dem Vorwurf einer „Einmischung“ in fremde Arbeitsbereiche aus dem Weg gehen, wenn Sie den Datenschutzbeauftragten ansprechen. Er ist auch gegenüber
der Unternehmensleitung zur Verschwiegenheit bezüglich Ihres Namens verpflichtet. Sie brauchen also keine Befürchtung zu haben, dass er einen Vorfall unter Ihrem Namen weitergibt.

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.

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.

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 deren Löschungsfrist.

Für dieses Löschkonzept 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.

Die Pflicht zu löschen gilt für alle Speicherorte wie für E-Mail-Accounts oder Webserver und natürlich auch für die gedruckten Fassungen dieser elektronischen Daten.

Den Löschpflichten gegenüber stehen die gesetzlichen Aufbewahrungsfristen, zum Beispiel für das Finanzamt. Während also Zeugnisse eines Bewerbers nach sechs Monaten gelöscht werden müssen, bleibt dessen Adresse auf seiner Reisekostenabrechnung für zehn Jahre gespeichert. Allerdings muss der Zugriff auf die Information in dieser Zeit eingeschränkt werden; das heißt, dass
im Tagesgeschäft oder für andere Zwecke der Zugriff auf diese Reisekostenabrechnung nicht mehr möglich ist.

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

Betroffenenrechte

Die Datenschutzgrundverordnung 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 der Person auf Anforderung diese Daten in einem „strukturierten, gängigen, maschinenlesbaren und inter-operablen Format“ bereitstellen oder einem anderen Anbieter übermitteln (Art. 20 DSGVO).

Fazit

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.

Datenverarbeitung durch Dienstleister – Auftragsdatenverarbeitung

In der heutigen Wirtschaft ist es unvermeidlich, dass Unternehmen personenbezogene Daten an Zulieferer und sonstige Dienstleister (wie Steuerberater, 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.

Datenverarbeitung im Ausland

Innerhalb des Europäischen Wirtschaftsraums (Europäische Union sowie Island, Liechtenstein und Norwegen) ist durch die Europäische Datenschutzgrundverordnung (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-Com-puting-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 Ihren 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

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 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. Die Meldung an die Aufsichtsbehörde muss innerhalb von 72 Stunden erfolgen, nachdem irgendein Mitarbeiter von dem Vorfall erfahren hat.

Auf Ihre Kenntnis kommt es also im Zweifel an. Nur in Ausnahmefällen kann die Geschäftsleitung mit ihrem Anwalt eine Verlängerung dieser Meldefrist erwirken. Auch das muss allerdings der Aufsichtsbehörde innerhalb der 72 Stunden mitgeteilt und begründet werden.

Fazit

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 Arbeitsanweisung geregelt werden.

HAFTUNG BEI DATENSCHUTZVERSTÖßEN

Grundsätzlich haftet 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. Aber 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.
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.

Für leicht fahrlässige rechtswidrige Datenverarbeitungen müssen Sie dem Arbeitgeber gegenüber nicht einstehen.

Handeln Sie allerdings sehr nachlässig oder sogar absichtlich, dann steigert sich Ihre Haftung mit Zunahme Ihres Verschuldens. 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.

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:

Bsp. 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.

Fazit

Datenschutzverstöße durch Mitarbeiter im Unternehmen können vor allem Schadensersatzpflichten und Bußgelder bis hin zu strafrechtlichen Verurteilungen nach sich ziehen. Schadensersatzpflichten treffen also, je nach Verschuldensgrad, nicht nur das Unternehmen, sondern auch den Mitarbeiter, der den Verstoß begangen hat.

Zudem drohen ihm arbeitsrechtliche Maßnahmen bis hin zur außerordentlichen Kündigung sowie Bußgelder und gegebenenfalls Strafverfahren.