KOMPLETT ÜBERARBEITETE AUFLAGE (DSGVO)

DATENSCHUTZ GANZ KURZ

Was Beschäftigte unbedingt wissen sollten

STIFTUNG DATENSCHUTZ

BvD e.V.
DATENSCHUTZ GESTALTEN

DATENSCHUTZ GESTALTEN

DER BERUFSVERBAND DER DATENSCHUTZ-BEAUFTRAGTEN DEUTSCHLANDS (BVD) E.V.

Datenschutzbeauftragte sorgen dafür, dass in Wirtschaft und Verwaltung die aktuellen Datenschutzbestimmungen eingehalten und die Abläufe zur Verarbeitung von personenbezogenen Daten gesetzeskonform geregelt sind.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. vertritt die Interessen von über 1.400 betrieblichen und behördlichen Datenschutzbeauftragten. Der Verband tritt dafür ein, Datenschutz stärker im Bewusstsein der Öffentlichkeit zu verankern – unter anderem mit dem Datenschutz Medienpreis (DAME) und der Initiative „Datenschutz geht zur Schule“ (DSgzS).

Mit Politik, Wirtschaft und den Aufsichtsbehörden von Bund und Ländern entwickelt der BvD-Datenschutz beständig als Wegbereiter für die digitale Zukunft weiter. Denn nur wer Daten von Kunden und Partnern erkennbar schützt, gewinnt Vertrauen und kann so Marken und Unternehmensimage stärken.

EINFÜHRUNG

Wenn Sie in Ihrem Unternehmen, Ihrer Praxis oder in jeder anderen Organisation mit personenbezogenen Daten arbeiten, müssen Sie sich mit den Grundregeln des Datenschutzes auskennen und mit den wesentlichen Pflichten, die sich daraus ergeben. Das betrifft Mitglieder der Geschäftsleitung ebenso wie Beschäftigte in allen Bereichen und in verschiedensten Anstellungsverhältnissen, auch wenn Sie nur gelegentlich mit personenbezogenen Daten arbeiten.

Diese Broschüre soll Ihnen dabei helfen, indem sie die wichtigsten Punkte unkompliziert und praxisnah darstellt. Wir haben bewusst darauf verzichtet, die genauen gesetzlichen Vorschriften aufzuführen – solch detaillierte Kenntnisse benötigen nur die Geschäftsführung, Datenschutzbeauftragte und Vorgesetzte, die regelmäßig und in großem Umfang mit personenbezogenen Daten arbeiten. Deren Aufgabe ist es auch, konkrete Arbeitsanweisungen für Ihren Betrieb herauszugeben. Diese Broschüre soll die betriebsspezifischen Datenschutzregelungen ergänzen.

Übrigens: Auch wenn diese Broschüre durchgehend von „Unternehmen“, „Geschäftsführern“ und „Beschäftigten“ spricht, gelten die Hinweise genauso auch für Vereine, Vorstände und andere Organisationen und Personen.

WELCHE GESETZE REGELN DEN DATENSCHUTZ?

Die wichtigsten Gesetze für den Datenschutz sind die Europäische **Datenschutz-Grundverordnung** (DSGVO) und das ergänzende neue **Bundesdatenschutzgesetz** (BDSG). Sie sind neben vielen weiteren Materialien abrufbar über die Informationsplattform der Stiftung Datenschutz zur Umsetzung der EU-Datenschutzreform unter www.stiftungdatenschutz.org/DSGVO-Info.

Die DSGVO gilt von Mai 2018 an unmittelbar in allen EU-Mitgliedsstaaten. Diese können sich ergänzende eigene Regelungen geben. Für Deutschland wurde das alte Bundesdatenschutzgesetz durch ein neues Bundesdatenschutzgesetz ersetzt. In diesem Begleitgesetz finden sich u.a. **Sonderregelungen für die Verarbeitung von Beschäftigtendaten, für die Videoüberwachung und für die Zahlungseinschätzung von Schuldnern (Scoring)**.

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

WOZU BRAUCHT ES DATENSCHUTZ?

Der Datenschutz ermöglicht das Grundrecht, dass jeder Mensch grundsätzlich selbst entscheiden können soll, welche seiner persönlichen Daten wem wann zugänglich sein sollen. Dieses Grundrecht wird durch den Datenschutz ermöglicht. Datenschutz soll nicht die Daten an sich schützen, sondern stets die Person, auf die sich die Daten beziehen.

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.

Personenbezogene Daten werden an vielen Stellen im Unternehmen verarbeitet: natürlich in der Personalabteilung (Mitarbeiter- und Bewerbungsdaten), aber auch im Einkauf (Lieferanten), im Vertrieb (Kunden), in der IT-Abteilung... Diese Daten dürfen nur für betriebliche Zwecke verwendet werden. Die Geschäftsführung ist verpflichtet, die entsprechenden Anweisungen herauszugeben und aktuell zu halten sowie die Beschäftigten darüber zu belehren und auf das Datengeheimnis zu verpflichten.

Viele Unternehmen bestellen auch einen Datenschutzbeauftragten. (Wenn sie regelmäßig zehn oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, sind sie dazu verpflichtet.)

Bei Verstößen im Umgang mit personenbezogenen Daten drohen – neben den Nachteilen für die betroffenen Personen – Schadensersatzforderungen und Bußgelder; der Ruf des Unternehmens bei Kunden, Lieferanten und in der Öffentlichkeit kann nachhaltigen Schaden nehmen.

WAS SIND EIGENTLICH PERSONENBEZOGENE DATEN?

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

- Unmittelbar zuzuordnen: Name, eventuell Funktion, wenn es zum Beispiel nur eine IT-Leiterin im Unternehmen gibt.
- Mittelbar zuzuordnen: Personalnummer, IP-Adresse

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

Darüber hinaus gibt es sensitive personenbezogene Daten, die noch strenger geschützt sind: Das sind Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der geschlechtlichen Orientierung 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 sensitiven Daten immer besonders fachkundiger Rat eingeholt werden.

WER IST FÜR DEN DATENSCHUTZ IM BETRIEB VERANTWORTLICH?

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

DIE UNTERNEHMENSLEITUNG SCHAFFT DIE RAHMENBEDINGUNGEN

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

MITARBEITERINNEN UND MITARBEITER WENDEN DIE ANWEISUNGEN AN

Praxisfälle

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

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

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

Daumenregel

Manchmal liegt es auf der Hand, manchmal ist es unklar, ob die eigene Datenverarbeitung datenschutzrechtlich zulässig ist. Hier könnte Ihnen die **Daumenregel** 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 BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Das Unternehmen muss einen betrieblichen Datenschutzbeauftragten stellen, wenn es **in der Regel zehn Personen oder mehr ständig mit der automatisierten Verarbeitung** personenbezogener Daten beschäftigt. Aufgabe des Datenschutzbeauftragten ist es, Geschäftsleitung und Beschäftigte hinsichtlich datenschutzkonformer Datenverarbeitung zu beraten. Die **Aufgabe, den Datenschutz sicherzustellen**, hat der Beauftragte dagegen **nicht**. Diese Aufgabe liegt bei der Unternehmensleitung und bei den Mitarbeitern.

Als unabhängiger und zur Verschwiegenheit verpflichteter Kontrolleur steht der Datenschutzbeauftragte aber als Ansprechpartner für alle Beschäftigten zur Verfügung. **Jede Meldung zu datenschutzrelevanten Umständen im Unternehmen wird er vertraulich bearbeiten.** Sollten Sie Fragen zum Datenschutz haben, können Sie sich also nicht nur an Ihren Vorgesetzten wenden, sondern jederzeit auch den betrieblichen Datenschutzbeauftragten ansprechen, ohne befürchten zu müssen, dass sich das für Sie nachteilig auswirkt.

DIE DATENSCHUTZAUFSICHTSBEHÖRDE BERÄT, KONTROLLIERT UND VERHÄNGT EVENTUELL BUßGELDER

Für jedes Unternehmen gibt es eine zuständige Behörde, die den Datenschutz im Unternehmen überwachen soll und vor allem auf Anzeigen und Beschwerden von Betroffenen reagiert. Für die meisten Unternehmen ist diese Behörde der oder die Landesbeauftragte für den Datenschutz (in Bayern das Landesamt für Datenschutzaufsicht). Die Bundesbeauftragte für den Datenschutz ist im wirtschaftlichen Bereich allein für die Unternehmen der Telekommunikations- und Postbranche zuständig.

Der **Bußgeldrahmen** ist mit der Datenschutz-Grundverordnung erheblich erhöht worden. Lag bisher der Maximalbetrag bei 300.000 Euro pro Fall, sind Unternehmen nun bei schwersten Datenschutzverstößen von einem Bußgeld von bis zu 20 Mio. Euro oder von bis zu vier Prozent ihres weltweiten Jahresumsatzes bedroht.

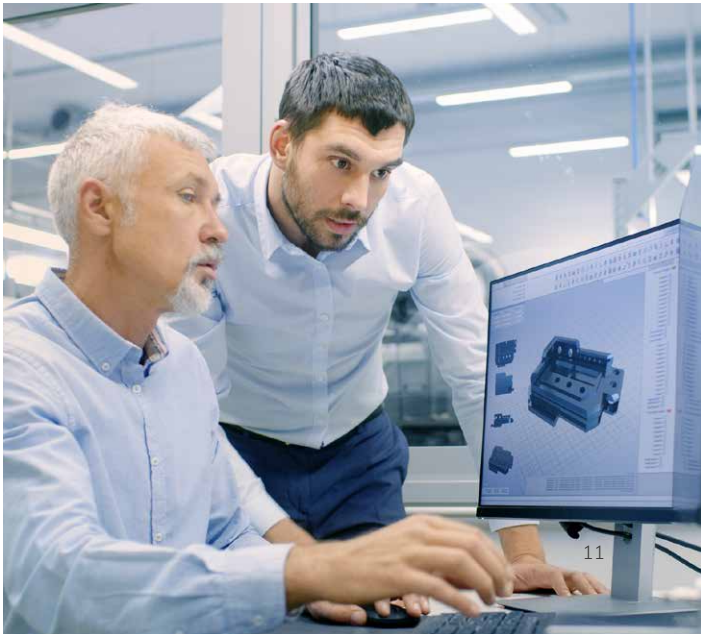
VIER PFLICHTEN FÜR DEN DATENSCHUTZ

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

- Die Datenverarbeitung muss durch eine Rechtsgrundlage überhaupt **erlaubt** sein.
- Die Betroffenen müssen über die Verarbeitung ihrer Daten **informiert** sein.
- Die Datenverarbeitung muss **sicher** erfolgen.
- Die Daten müssen **gelöscht** werden, sobald sie nicht mehr benötigt werden.

IST DIE DATENVERARBEITUNG ERLAUBT?

Ohne dass eines der gesetzlichen Erlaubnisse erfüllt ist (**Einwilligung, Rechtsvorschrift, Betriebsvereinbarung, Vertrag oder Vertragsvorbereitung auf Wunsch des Kunden, überwiegendes Interesse des Unternehmens**), darf das Unternehmen keine personenbezogenen Daten verarbeiten. Entscheidend ist dabei immer, ob die Kundendaten auch tatsächlich erforderlich sind, um den konkreten Zweck zu erreichen.



Beispiele für erlaubte Datenverarbeitung

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

Ihre Prüffrage

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

IST DIE BETROFFENE PERSON ÜBER DIE DATENVERARBEITUNG INFORMIERT?

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

Ihre Checkliste zur Informationspflicht

Ist die betroffene Person hinreichend informiert über

- ☐ den vollständigen Namen und
- ☐ die vollständige Adresse Ihres Unternehmens,
- ☐ die vollständige Adresse des Datenschutzbeauftragten (wenn es einen gibt),
- ☐ alle Zwecke, für die die Daten der betroffenen Person verwendet werden, einschließlich der Rechtsgrundlage der Verarbeitung und der „berechtigten Interessen", falls die Erlaubnis aus einer Interessenabwägung resultiert,
- ☐ die Kategorien von Empfängern der Daten, falls die Datenweitergabe geplant ist,
- ☐ eine eventuelle Verarbeitung der Daten außerhalb des europäischen Wirtschaftsraums,
- ☐ die zeitliche Dauer, in der die Daten ungelöscht und uneingeschränkt verwendbar im Unternehmen verbleiben,
- ☐ ihre Betroffenenrechte, also ihre Widerrufsrechte, ihre Beschwerderechte oder die Tatsache, dass eine Entscheidung – zum Beispiel über eine Kreditvergabe – nach automatischen Berechnungen direkt von einem IT-System getroffen wird?

ERFOLGT DIE VERARBEITUNG DER DATEN SICHER?

Unternehmen wie Beschäftigte müssen dafür Sorge 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.

Es ist daher arbeitsvertragliche **Nebenpflicht, sowohl die Informationen über natürliche Personen als auch vertrauliche Firmeninformationen vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen**.

DATENSICHERHEITSREGELN

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

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

Kommunikation
Seien Sie grundsätzlich bei der Weitergabe von Daten vorsichtig. Achten Sie stets sorgfältig darauf, die **richtige E-Mail-Adresse und Faxnummer** einzugeben. Und überprüfen Sie auch, ob die Person hinter der E-Mail-Adresse oder Faxnummer 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** zu informieren (siehe Abschnitt „Verhalten bei Datenlecks“).

Verschlüsselung, Passwörter
Meist geben Unternehmen entsprechende Arbeitsanweisungen heraus. Andernfalls halten Sie sich am besten an die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.bund.de), dessen Empfehlungen übrigens auch für den privaten Bereich sinnvoll sind. **Beim Verlassen des Rechners ist dieser zu sperren** (bei Windows-Rechnern: WINDOWS-Taste + L, bei Mac-Rechnern: Control + 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 betrieblichen 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.

Ihre Prüffrage

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

DATEN AUFBEWAHREN, LÖSCHEN ODER DEN ZUGRIFF EINSCHRÄNKEN?

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

Beispiel

So ist zulässig, bestimmte Bereiche des Betriebs, wie den Eingang zum Lager, per Videokamera zu überwachen. Doch auf die Aufzeichnungen der Videokameras darf nur ein ganz eingeschränkter Personenkreis zugreifen, der Zugriff muss protokolliert werden und nach Ablauf von wenigen Tagen müssen die Aufnahmen durch Überschreiben gelöscht werden. Videobilder dürfen aber nicht dafür genutzt werden, zum Beispiel über Wochen hinweg das Kommen und Gehen einzelner Mitarbeiter zu ermitteln.

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

Beispiel

Bewerbungsunterlagen müssen sechs Monate nach der Besetzung der Stelle gelöscht werden, d.h. die

Unterlagen sind an die betroffenen Personen zurückzuschicken oder zu vernichten. Reisekostenabrechnungen für Bewerbungsgespräche mit der Adresse der Bewerber müssen jedoch für die Buchhaltung zehn Jahre lang aufbewahrt werden.

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

Den Löschpflichten gegenüber stehen die gesetzlichen Aufbewahrungsfristen, zum Beispiel für das Finanzamt. Während also Zeugnisse der sich bewerbenden Person nach sechs Monaten gelöscht werden müssen, bleibt ihre Adresse auf der Reisekostenabrechnung noch für zehn Jahre gespeichert. Allerdings muss der Zugriff auf diese Information in dieser Zeit eingeschränkt werden, sodass ein Zugriff im Tagesgeschäft oder für andere Zwecke nicht mehr möglich ist.

VERHALTEN BEI DATENLECKS

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

Ihre Vorgehensweise bei einer Datenschutzverletzung

Wenn Sie einen Datenschutzvorfall erkennen, wenden Sie sich **sofort** an Ihren Vorgesetzten und an den betrieblichen Datenschutzbeauftragten. Erstellen Sie einen kurzen Bericht (Welche Daten sind abgeflossen oder waren im Zugriff? Wie ist es dazu gekommen? Welche Folgen vermuten Sie?) und senden Sie diesen an Ihren Vorgesetzten.

ÜBER DIE STIFTUNG DATENSCHUTZ

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

Stiftung Datenschutz
Frederick Richter (V.i.S.d.P.)

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

Version 1.0, Stand Mai 2018