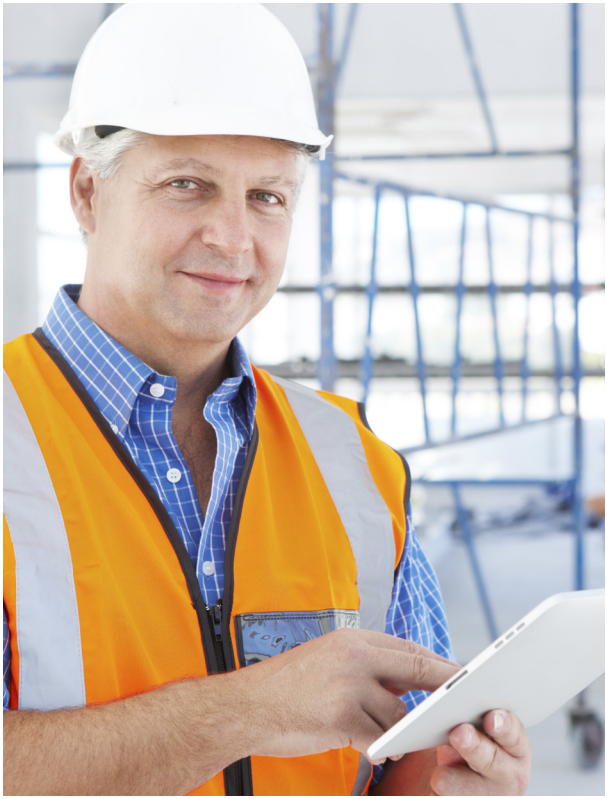


DATENSCHUTZ GANZ KURZ

WAS BESCHÄFTIGTE WISSEN SOLLTEN

STIFTUNG DATENSCHUTZ

EINFÜHRUNG

Wenn Sie in Ihrem Betrieb mit personenbezogenen Daten arbeiten, ist diese Broschüre für Sie – egal, wie groß Ihr Unternehmen ist. Der datenschutzgerechte Umgang mit personenbezogenen Daten ist in jedem Unternehmen Pflicht für jeden Mitarbeiter – von der Geschäftsleitung bis zum Praktikanten. 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. Sie ist allgemein gehalten und so knapp wie möglich gefasst.

Wenn Sie etwas mehr wissen wollen, nehmen Sie die ebenfalls von der STIFTUNG DATENSCHUTZ herausgegebene Broschüre „Was müssen Beschäftigte unbedingt über den Datenschutz wissen?“ zur Hand.

Bitte informieren Sie sich auch über betriebseigene Merkblätter oder Arbeitsanweisungen zum Datenschutz, da diese unter Umständen betriebsspezifische Datenschutzregelungen enthalten.

GRUNDLAGEN

Der Datenschutz soll den Einzelnen vor Nachteilen schützen, die durch übermäßigen Umgang mit ihn betreffenden Informationen entstehen können. Im Kern geht es um Entscheidungsfreiheit: Jeder soll selbst entscheiden können, wem wann welche seiner persönlichen Daten bekannt werden. Man spricht vom „Recht auf informationelle Selbstbestimmung".

Die Rechtsvorschriften zum Umgang mit Daten finden sich hauptsächlich im Bundesdatenschutzgesetz (BDSG). Daneben gibt es noch Sondervorschriften, zum Beispiel für den Telekommunikationsbereich, den Versicherungsbereich und das Gesundheitswesen. Wir können uns hier nur mit den allgemeinen Grundsätzen befassen.

Die Gesetze und Vorschriften zum Datenschutz schützen nur Daten, die sich auf eine konkrete Person beziehen, sogenannte „personenbezogene Daten".

„Daten" sind dabei alle konkreten Angaben, z. B. Adresse und Geburtsdatum, Bankverbindung, persönliche Vorlieben oder gesundheitliche Informationen.

„Personenbezogen" sind diese Angaben, sobald es um einen konkreten Menschen geht. Dafür reicht es aus, wenn der jeweilige Mensch zwar nicht mit Namen genannt ist, aber sein Name leicht ermittelt werden kann. So enthält bereits die Aussage „der Leiter der Einkaufsabteilung ist krank" personenbezogene Daten.

DATENSCHUTZ IM BETRIEB

Datenschutz ist wichtig für das Vertrauen von Kunden, Lieferanten und Beschäftigten in das Unternehmen. Als in der vergangenen Jahren schwere Datenschutzverstöße in großen deutschen Unternehmen bekannt wurden, hat dies deren Ansehen sehr geschadet. Nicht zuletzt deshalb sollten alle Beschäftigten stets die Anforderungen des Datenschutzes beachten. Datenschutz ist auch ein Wettbewerbsfaktor!

Personenbezogene Daten werden an vielen Stellen im Betrieb verarbeitet: Natürlich in der Personalabteilung (Mitarbeiter, Bewerber), aber auch im Vertrieb (Kundendatenbanken), im Einkauf (Lieferanten), in der IT-Abteilung... Ob diese Daten elektronisch oder auf Papier vorliegen, spielt für den Datenschutz keine Rolle.

Diese Daten dürfen nur für betriebliche Zwecke verwendet werden. Sie persönlich sind verpflichtet, sie geheim zu halten. Die Geschäftsleitung ist dafür verantwortlich, Sie auf das „Datengeheimnis" zu verpflichten, zum Beispiel im Rahmen des Arbeitsvertrags.

Für Führungskräfte, Betriebsratsmitglieder und die Personalabteilung gelten noch strengere Geheimhaltungspflichten, denn sie arbeiten mit besonders sensiblen Informationen über Kollegen und Bewerber.

Bei Verstößen gegen die Datenschutzvorschriften muss das Unternehmen mit Schadensersatzforderungen und Bußgeldern rechnen. Arbeitsrechtliche Maßnahmen (z. B. Abmahnungen) sind möglich, wenn Beschäftigte fahrlässig gehandelt haben.

ERLAUBT ODER VERBOTEN?

Die Nutzung personenbezogener Daten ist oft erforderlich, damit ein Unternehmen überhaupt seine Produkte und Dienstleistungen herstellen und verkaufen kann. Daher erlaubt das Gesetz die Verarbeitung personenbezogener Daten unter bestimmten Bedingungen.

Zulässig ist die Datenverarbeitung nur,

- wenn die Datenverarbeitung durch gesetzliche Vorschrift erlaubt ist (z. B. bei der Vorbereitung von Verträgen, für Werbezwecke, für die Strafverfolgung),
- oder wenn die Datenverarbeitung durch eine Vorschrift angeordnet ist (z. B. Weitergabe von Lohndaten an das Finanzamt),
- oder wenn die betroffene Person in die Datenverarbeitung eingewilligt hat (z. B. freiwillige Aufnahme in eine Geburtstagsliste).

Prüffrage 1
Gibt es eine Vorschrift oder eine Einwilligung, die erlaubt, dass ich Informationen zu einer Person aufbereite, weitergebe oder anderweitig nutze?

Prüffrage 2
Der Betroffene soll in die Verarbeitung seiner Daten einwilligen. Weiß er,

- welche Daten
- zu welchem Zweck
- von wem verarbeitet werden sollen?

Hat er ein Widerspruchsrecht und kann er die datenverarbeitenden Unternehmen erreichen?

Für die Verarbeitung von besonders sensiblen Daten, die zum Beispiel die Gesundheit betreffen, gibt es spezielle Vorschriften.

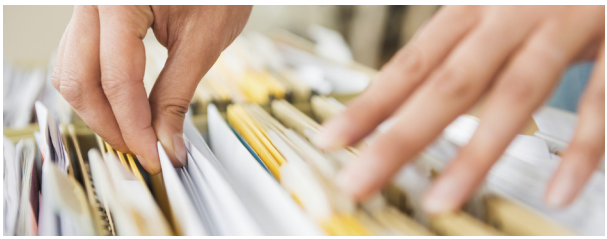
AUFHEBEN ODER LÖSCHEN?

Ihr Unternehmen muss sich auch darum kümmern, was in der Zukunft mit abgeschlossenen Vorgängen passiert, die personenbezogene Daten enthalten.

Grundsätzlich müssen personenbezogene Daten gelöscht werden, sobald der ursprüngliche Zweck, zu dem sie gespeichert wurden, erfüllt oder entfallen ist.

Ausnahmsweise können spezielle Aufbewahrungspflichten bestehen; dann dürfen die betroffenen Daten nicht gelöscht werden, obwohl sie das Unternehmen eigentlich nicht mehr braucht. Das Unternehmen ist dann verpflichtet, die Daten aufzubewahren; es muss sie aber sperren. Durch ein solches „Wegschließen" der betroffenen Daten (physisch oder elektronisch) soll sichergestellt werden, dass der Zugriff für andere Zwecke ausgeschlossen ist.

Beispiel
Rechnungsunterlagen müssen 10 Jahre, manchmal sogar länger, aufbewahrt werden, damit die Möglichkeit einer Betriebsprüfung erhalten bleibt.



Fazit
Das Unternehmen ist verpflichtet, Regelungen dazu zu treffen, ob und wann welche Daten zu löschen sind und welche Daten aufbewahrt, aber gesperrt werden müssen. Keinesfalls jedoch sollten Sie im Unternehmen vorhandene Daten einfach ohne Rückfrage löschen.

HINWEISE FÜR DIE PRAXIS

Sie sind in Ihrem jeweiligen Arbeitsbereich durch den Datenschutz verpflichtet, nicht nur vertrauliche Firmeninformationen, sondern auch Informationen über Personen vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen. Um Pannen bei der Verwendung und Weitergabe personenbezogener Daten zu vermeiden, dürfen Sie folgende Punkte bitte niemals außer Acht lassen:

Papierakten
Dokumente mit personenbezogenen Daten dürfen nicht im normalen Müll entsorgt werden, sondern müssen entweder mit einem Aktenvernichter vernichtet oder in spezielle Datenabfallbehälter gegeben werden.

Kommunikation
Seien Sie grundsätzlich vorsichtig bei der Weitergabe von Personendaten. Achten Sie darauf, dass Ihre E-Mails korrekt adressiert sind. Nutzen Sie das Feld „Blindkopie" (BCC), um die Empfänger voreinander zu verbergen. Schützen Sie angehängte Dateien wenn nötig durch Passwörter oder Verschlüsselung. Überprüfen Sie bei der Faxübermittlung immer noch einmal die eingegebene Nummer. Stellen Sie bei der Übermittlung von besonders wichtigen personenbezogenen Daten (vor allem Personaldaten, Gesundheitsdaten) sicher, dass diese vom Empfänger persönlich entgegengenommen werden. Versenden Sie geheimhaltungsbedürftige Daten im Zweifel nur verschlüsselt oder per Post.

Datentransport
Personenbezogene Daten sind nur auf firmeneigenen portablen Datenträgern (USB-Stick, Festplatte) und eventuell zusätzlich verschlüsselt zu transportieren. Fremde Datenträger von außen sollten niemals ungeprüft verwendet werden.

Verschlüsselung, Passwörter
Verwenden Sie für Passwörter eine Kombination aus Buchstaben, Zahlen und Sonderzeichen und wechseln Sie sie regelmäßig. Die Datensicherheitsbehörde des Bundes, das Bundesamt für Sicherheit in der Informationstechnik gibt dazu Ratschläge, die auch im privaten Bereich nützlich sind (www.bsi-fuer-buerger.de/Passwoerter).

Computersperre
Sperren Sie Ihren Rechner immer, wenn Sie Ihren Arbeitsplatz verlassen. Die Sperre sollte sich nur mit einem Passwort wieder aufheben lassen. Auch diese Passwörter sollten nach der oben erwähnten Regel gebildet werden. Zusätzlich sollte sich nach vorgegebener Zeit die Bildschirmsperre automatisch einschalten, so dass auch bei ungeplanten Abwesenheiten niemand einfach an Ihr Gerät gehen kann.

Schutz vor Mithören
Sorgen Sie dafür, dass Unbefugte keine Telefongespräche mitverfolgen können.

Telefonische Anfragen
Wenn Sie telefonisch um Auskünfte gebeten werden, prüfen Sie:

1) Ist der Anrufer der, der er zu sein vorgibt?
2) Ist der Anrufer berechtigt, die erfragten Informationen zu erhalten?

Lassen Sie sich eine Rückrufnummer geben und sprechen Sie bei Zweifeln mit Vorgesetzten.

Sprechen Sie Betriebsfremde, die sich unbegleitet im Unternehmen aufhalten, an und fragen Sie sie nach Identität und Anliegen.

Dürfen Datenbestände angereichert werden?
Das Anreichern von Datenbeständen bedeutet, dass bereits vorhandenen Informationen über Kollegen, Bewerber, Kunden- und Lieferantenbeschäftigte, Gäste oder andere Personen weitere neue Informationen hinzugefügt werden. Dies ist nur erlaubt, wenn es erforderlich und verhältnismäßig ist.

Beispiel
Ein Versandhändler darf Informationen zur Zahlungsfähigkeit „anreichern". Eine Personalabteilung darf aber keine Facebook-Informationen zu Bewerberunterlagen hinzufügen.

Was ist bei der Weitergabe von Daten an andere Unternehmen zu beachten?
Ein Unternehmen arbeitet heute meist nicht allein, sondern arbeitsteilig. Es schaltet Zulieferer und sonstige Dienstleister ein, z. B. Schreibbüros, Aktenvernichtungsunternehmen, Rechenzentren, IT-Dienstleister u. ä. Dabei werden in verschiedenen Situationen personenbezogene Daten auch an diese Fremdfirmen zur weiteren Bearbeitung weitergegeben. Die Fachleute nennen das Auftragsdatenverarbeitung. Das Gesetz verlangt in diesen Fällen, dass in einem schriftlichen Vertrag sichergestellt wird, dass der Dienstleister und dessen Beschäftigte die gesetzlichen Datenschutzregelungen einhalten. Ihr Unternehmen bleibt für die Daten weiterhin verantwortlich und muss daher auch prüfen, ob die Daten durch den Dienstleister ausreichend geschützt werden.

Offene Augen und Ohren
Wenn Sie von Datenschutzverstößen erfahren, informieren Sie Ihr Unternehmen sofort darüber. Am besten sprechen Sie den betrieblichen Datenschutzbeauftragten an. Er ist verpflichtet, Ihre Identität vertraulich zu behandeln. Vorgesetzte und Kollegen erfahren also nicht, dass Sie der Hinweisgeber sind.

Wie verhalte ich mich, wenn doch einmal Daten abhandenkommen?
Kein Unternehmen ist 100%ig sicher. Es wird in jedem Unternehmen irgendwann einmal einen Vorfall in der IT-Sicherheit oder ein „Datenleck" geben. Dann ist es das Wichtigste, Schaden abzuwenden - von den Personen, deren Informationen abhandengekommen sind und vom Unternehmen selbst.

Beispiele für sensiblen Umgang mit Personendaten

Daten von Kollegen/Mitarbeitern/Bewerbern:
- Geburtstagslisten besser ohne Geburtsjahr erstellen
- E-Mail-Verteilerlisten im Zweifel in BCC-Feld setzen

Daten von Kunden/Interessenten:
- Nutzung der Daten nur zu dem Zweck, zu dem sie gesammelt/gespeichert wurden (keine ungefragte Nutzung für Werbung, wenn nur für Abwicklung eines Liefervertrages gespeichert)

Wenn Datenträger – egal, ob Laptop oder Aktenordner – mit personenbezogenen Daten abhandengekommen sind, informieren Sie Vorgesetzte, betriebliche Datenschutzbeauftragte oder die Geschäftsleitung, zum Beispiel per E-Mail oder per Hauspost, notfalls auch mündlich. Möglicherweise gibt es auch eine Betriebsvereinbarung, die regelt, wie Sie sich verhalten und wen Sie informieren müssen.

IHRE ANSPRECHPARTNER FÜR DEN DATENSCHUTZ

Die Geschäftsführung

Die Unternehmensleitung ist für die Einhaltung der Datenschutzvorschriften im Betrieb verantwortlich. Sie muss alle Beschäftigten dazu verpflichten, bei ihrer jeweiligen Tätigkeit für das Unternehmen datenschutzkonform zu handeln. Für diese Verpflichtung wird meist eine Datenschutzarbeitsanweisung erteilt und von den Beschäftigten das Unterzeichnen einer Erklärung zur Verschwiegenheit verlangt.

Der Datenschutzbeauftragte Ihres Unternehmens

Wenn mehr als neun Beschäftigte in einem Betrieb ständig Personendaten automatisiert verarbeiten, muss das Unternehmen einen betrieblichen Beauftragten für den Datenschutz bestellen (dies kann auch eine externe Person sein, z. B. ein IT-Berater oder Rechtsanwalt). Der Datenschutzbeauftragte überprüft die Rechtmäßigkeit der betrieblichen Datenverarbeitungsvorgänge. Er berät die Geschäftsleitung und die Beschäftigten und steht bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten zur Verfügung. Sofern Sie sich mit einem Problem an den betrieblichen Datenschutzbeauftragten wenden, ist er der Geschäftsführung 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 gut an den betrieblichen Datenschutzbeauftragten.

Die Datenschutzaufsichtsbehörden

Die Landesbeauftragten für den Datenschutz kontrollieren als staatliche Aufsichtsbehörden die Einhaltung der Datenschutzvorschriften in den Betrieben (zuständig ist die Behörde desjenigen Bundeslandes, in dem das Unternehmen seinen (Haupt)-Sitz hat). Die Kontaktdaten aller Datenschutzaufsichtsbehörden finden Sie unter: https://stiftungdatenschutz.org/aufsichtsbehorden-im-datenschutz. Die Bundesbeauftragte für den Datenschutz ist nur für Telekommunikations- und Postunternehmen zuständig.

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