



Mitarbeiterinformation Datenschutz

Merkblatt zum Datenschutz für Mitarbeiter nach
DS-GVO und BDSG



WAS IST ... DATENSCHUTZ?



Liebe Kollegen,

das Thema Datenschutz betrifft Sie in zweifacher Hinsicht. Zum einen als Kunde oder Mitarbeiter, dessen Daten verarbeitet werden, zum anderen, weil Ihnen personenbezogene Daten Dritter bei Ihrer Tätigkeit zur Kenntnis gelangen. Das Datenschutzrecht erlaubt es Ihnen nur, personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten oder sonstigen Dritten auf Grundlage gesetzlicher Vorschriften und entsprechender interner Anweisungen zu verarbeiten. Die Wahrung der Vertraulichkeit ist eine arbeits- und datenschutzrechtliche Pflicht.

Rechtliche Grundlage hierfür ist die Datenschutz-Grundverordnung (DS-GVO). Sie hat zum Ziel, den Datenschutz in der EU zu modernisieren und zu vereinheitlichen. Die DS-GVO wird ergänzt durch ein neues Bundesdatenschutzgesetz (BDSG).

Der Zweck des Datenschutzes, den Einzelnen davor zu schützen, dass er im Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, erfordert ein verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch eine risikobewusste Nutzung von IT-Systemen und -Anwendungen. Diese Mitarbeiterinformation soll Ihnen einen Überblick über die Grundlagen des Datenschutzes geben und Sie über Ihre Rechte und Pflichten aufklären. In meiner Funktion als Datenschutzbeauftragter stehe ich Ihnen selbstverständlich in allen Zweifelsfragen zur Verfügung. Bitte wenden Sie sich vertrauensvoll an mich.

Ihr Datenschutzbeauftragter

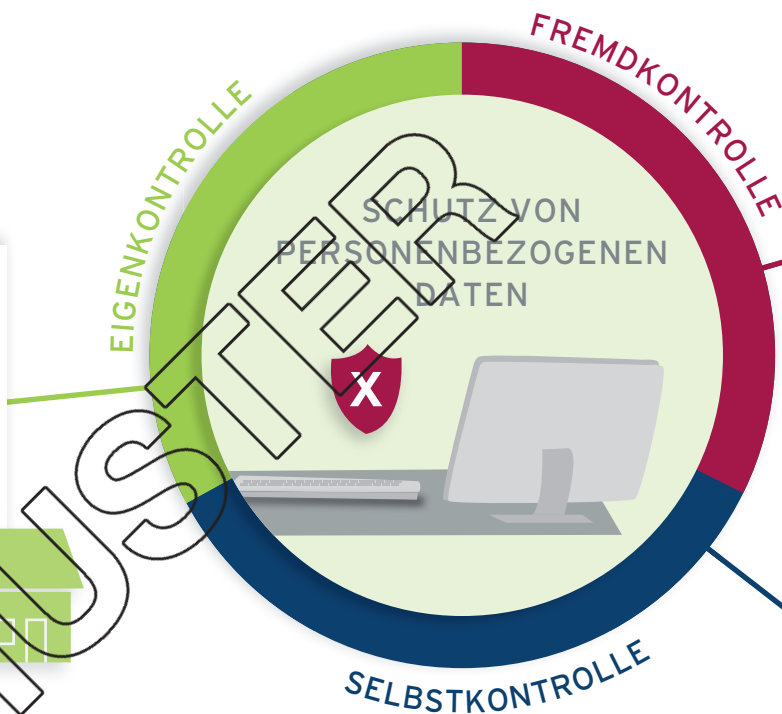
DATENSCHUTZ IM ÜBERBLICK

Die betroffene Person

... übt ihre Rechte aus

Sie kann Auskunft über gespeicherte Daten beantragen und ggf. Berichtigung, Löschung, Sperrung oder Portierung ihrer Daten erwirken.

» AB SEITE 16



Der Staat

... kontrolliert die Einhaltung
Die Datenschutz-Aufsichtsbehörde
kann unzulässige Verfahren bean-
standen, Bußgelder verhängen und
Strafanträge stellen.

» AB SEITE 6



MUSTER

Das Unternehmen

... hat die Verantwortung
dafür, dass die Verarbeitung
personenbezogener Daten nur ent-
sprechend dem Datenschutzrecht
erfolgt.

» AB SEITE 8

... organisiert den Datenschutz
Das Unternehmen macht die
Vorgaben, wie und unter welchen
Voraussetzungen personenbezoge-
ne Daten erhoben und verarbeitet
werden dürfen.

» AB SEITE 12

... sichert die Daten
Personenbezogene Daten
müssen vor unbefugtem
Zugriff, Verlust und
Zerstörung ausreichend
geschützt werden.

» AB SEITE 14

DIE BEDEUTUNG DES DATENSCHUTZES

Warum ist Datenschutz notwendig?

Die technologische Entwicklung der automatisierten Datenverarbeitung führt zu steigenden Gefahren des Datenmissbrauchs. Es fallen immer mehr Daten an, die nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können. Der Einzelne wird dadurch in seinen Persönlichkeits- und Freiheitsrechten beeinträchtigt, insbesondere wenn er nicht weiß, wer welche Daten über ihn hat, was dieser mit diesen macht und an wen er sie weitergibt.



Art. 1 Abs. 2 DS-GVO

„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“



Art. 4 Nr. 1 DS-GVO

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, [...] identifiziert werden kann;“





MERKSATZ

Jeder Mitarbeiter muss mit personenbezogenen Daten sorgfältig und achtsam umgehen!
(siehe Seite 7/8)

Was sind personenbezogene Daten?

Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimmbar natürliche Person.

Beispiele

ADRESSE	VERMÖGEN	 ARBEITSVERHALTEN	 BENUTZERKENNUNG
GEBURTSDATUM	BESITZ	PERSONALNUMMER	MASCHINENBEZOGENE
TELEFONNUMMER	GEHALT	ARBEITSERGEBNISSE	NUTZUNGSZEITEN
	FOTO		

Besonders sensitive Daten sind z.B. rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben sowie biometrische und genetische Daten. Ihre Verarbeitung ist nur unter strengen Regeln erlaubt, ihre Verwendung z.B. für Marketingzwecke in der Regel unzulässig.

Was sind die rechtlichen Grundlagen?

Wegen der Gefahren für das Persönlichkeitsrecht bedarf jede personenbezogene Datenverarbeitung einer rechtlichen Grundlage. Die Grundlagen des Datenschutzes sind europaweit durch die Datenschutz-Grundverordnung (DS-GVO) geregelt. Diese wird durch das Bundesdatenschutzgesetz (BDSG) ergänzt. Daneben gibt es bereichsspezifische Vorschriften. (siehe Seite 9)

Wen schützt die Datenschutz-Grundverordnung (DS-GVO)?

Die DS-GVO schützt natürliche Personen bei der Verarbeitung ihrer persönlichbezogenen Daten. Geschützt sind demnach Mitarbeiter, Kunden und Lieferanten oder deren Ansprechpartner. (siehe Seite 10) Der Schutzbedarf von Daten hängt von ihrem Verwendungszweck ab.

WER MUSS DIE DS-GVO BEACHTEN?



1. 2. 3. DATAKONTEXT DATAKONTEXT DATAKONTEXT

1. Private rechtliche Organisationen und Firmen, aber auch Personen, die personenbezogene Daten verarbeiten. Bsp: Selbstständige, Vereine, Produktions-, Handels- und Dienstleistungsunternehmen aber auch Anbieter sozialer Netzwerke.

2. Sonstige privatwirtschaftliche Organisationen, deren Geschäftszweck die Verarbeitung personenbezogener Daten für Fremde ist wie Service-Rechenzentren, Wirtschaftsuniversitäten, Markt- und Meinungsbroschüren, Adressenhandler, -broker und -verlage sowie wissenschaftliche Forschungseinrichtungen und Medien.

3. Öffentlich Stellen der Bundes- und der Länder, z.B. die Bundesländer oder die Kommunalverwaltungen.

DATAKONTEXT DATAKONTEXT DATAKONTEXT

KONTROLLE DURCH DEN STAAT

DATAKONTEXT DATAKON Datenschutz-Aufsichtsbehörden

Die Aufsichtsbehörde kontrolliert die Datenkontrollorganisation eines Unternehmens, die Zulässigkeit der Datenverarbeitung und die Beachtung der Betroffenenrechte, macht Auflagen und kann unter Umständen sogar ein unzulässiges Verfahren untersagen. Dazu hat sie Informations-, Betretens-, Besichtigungs-, Prüfungs- und Einsichtsrechte. Zudem kann die Aufsichtsbehörde erhebliche Bußgelder verhängen und Sanktionen stellen.

Die europäischen Aufsichtsbehörden stimmen sich in ihren Datenschutzausschüssen über die einheitliche Anwendung der DS-GVO ab.

TAKONTEXT DATAKONTEXT DA TAKONTEXT DATAKONTEXT



DIE VERANTWORTUNG DES UNTERNEHMENS

Das Unternehmen hat die Verantwortung für den Datenschutz. Die DS-GVO spricht deshalb vom Verantwortlichen. Dienstleister, die lediglich Datenverarbeitung im Auftrag betreiben (z.B. Service-Rechenzentren, Entsorger) werden der verantwortlichen Stelle zugeordnet.



Art. 5 DS-GVO

Grundsätze der Verarbeitung personenbezogener Daten

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datensparsamkeit
- Rechtfertigung
- Speicher(dauer)begrenzung
- Integrität und Vertraulichkeit

Wann müssen Unternehmen die DS-GVO beachten?

Die DS-GVO und das BDSG greifen überall dort, wo personenbezogene Daten verarbeitet werden, sei es mittels IT oder in strukturierten Datenmengen, wie z.B. Karteikarten oder Akten. Das betrifft die Daten von Mitarbeitern genauso wie die von Kunden oder Lieferanten. Die Zulässigkeit der Verarbeitung von Mitarbeiterdaten ist nicht auf Daten des Intranet beschränkt. Jede Information über ein in Mitarbeiter datenschutzkonform erlangt und erfasst werden.

Datenschutzmanagement

Die DS-GVO fordert von Unternehmen in Abhängigkeit von Risiko für die betroffenen Personen ein Datenschutzmanagement. Technische und organisatorische Maßnahmen müssen umgesetzt, regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Beachtung der Grundsätze der Datenverarbeitung und des Datenschutzmanagement müssen vom Unternehmen nachgewiesen werden.

Wer trägt die Verantwortung im Unternehmen?

Das Unternehmen handelt über seine Leitung, also den Vorstand oder die Geschäftsführung. Diese trägt die Verantwortung für die Etablierung des Datenschutzes.

Für die Umsetzung des Datenschutzes sind die Leiter und Mitarbeiter der Fachbereiche verantwortlich. Sie müssen die rechtlichen Vorgaben und Regelungen des Unternehmens umsetzen. Deshalb sollen Unternehmen die mit der Datenverarbeitung betrauten Personen über die Vorschriften der DS-GVO und des BDSG und gegebenenfalls über weitere relevante Datenschutzvorschriften informieren. Zudem sollten sie vor Beginn ihrer Tätigkeit auf die Vertraulichkeit verpflichtet werden. Für Mitarbeiter von Dienstleistern der Auftragsverarbeitung ist diese Verpflichtung nach der DS-GVO obligatorisch.

WANN IST DATENVERARBEITUNG ZULÄSSIG?

Jede Verarbeitung von personenbezogenen Daten bedarf einer gesetzlichen Rechtfertigung. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.



oder



oder



Erlaubnis durch die DS-GVO

Wesentliche Erlaubnisse zur Verarbeitung personenbezogener Daten nach der DS-GVO sind:

- ▶ die Einwilligung. Die Einwilligung muss freiwillig und nachweisbar sein. Ein Vertrag darf nicht zusätzlich von einer Einwilligung abhängig gemacht werden (Kopplungsverbot)
- ▶ zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen
- ▶ zur Erfüllung einer rechtlichen Verpflichtung
- ▶ zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen der betroffenen Person überwiegen
- ▶ bei Datenverarbeitung zu neuen Zwecken, wenn diese mit dem ursprünglichen Zweck kompatibel sind.

Erlaubnis durch das BDSG

Das BDSG ergänzt die Erlaubnistatbestände der DS-GVO

- ▶ zur Verarbeitung im Beschäftigungskontext
- ▶ zur Videoüberwachung
- ▶ zur Datenübermittlung an Auskunftsteilen
- ▶ zum Scoring

Erlaubnis durch andere Rechtsvorschriften

Auch außerhalb des BDSG gibt es Rechtsvorschriften, die es gestatten oder sogar dazu verpflichten können, Daten zu verarbeiten. Von hoher praktischer Relevanz sind beispielsweise das Steuer- und Sozialversicherungsrecht für die Entgeltabrechnung. Für die Verarbeitung von Personaldaten sind abgeschlossene Betriebs- oder Dienstvereinbarungen vorrangig.

FORMEN DES UMGANGS MIT PERSONENBEZOGENEN DATEN

Die DS-GVO gilt für die automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten in einem Dateisystem (z.B. Karteikarten).

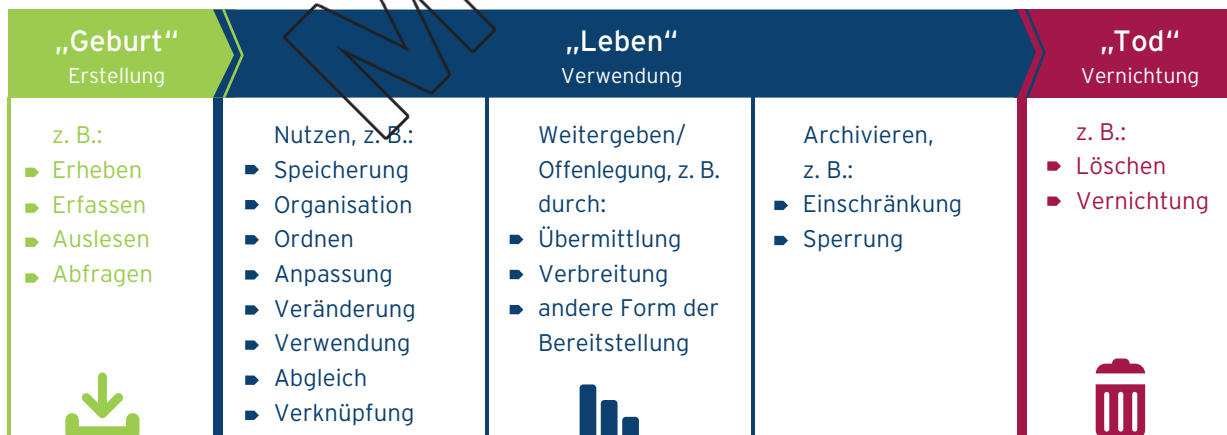


MERKSATZ

Jede Datenverarbeitung muss durch die DS-GVO, das BDSG, eine andere Rechtsvorschrift oder durch Einwilligung der betroffenen Person gestattet sein.

Der Begriff der Verarbeitung im Sinne der DS-GVO erfasst jeden Vorgang des Umgangs mit personenbezogenen Daten. Die Verarbeitung beginnt bei der Datenbeschaffung beim Betroffenen (z.B. durch schriftliche oder mündliche Befragung) oder bei Dritten (z.B. Kauf von Adressen bei einem Adresshändler) und reicht über deren Verwendung (z.B. durch Auswertung oder Weitergabe) bis hin zu deren Unkenntlichmachung.

DATA-LIFE-CYCLE



BEISPIELE: ZULÄSSIG ODER NICHT?

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen speichert seine Kundendaten zur Abwicklung eines Kaufvertrags und zur Prüfung möglicher Gewährleistungsansprüche.

> Zulässig,

weil die Datenverarbeitung auf Grund eines bestehenden Vertragsbeziehungs erfolgt.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen erschickt Mätlings per Post an seinen bestehenden Kundenstamm, um ein neu eingeführtes Produkt zu bewerben.

> Zulässig,

weil Kundendaten auch für Zwecke der Werbung verwendet werden dürfen.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Nutzung von Daten für eigene Werbezwecke, obwohl der Kunde erklärt hat keine Werbung erhalten zu wollen.

> Unzulässig,

weil bei einem **Werbewiderspruch** die Daten für diesen Zweck nicht genutzt werden dürfen.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen übermietet die Lohn- und Einkommensdaten seiner Mitarbeiter an das Finanzamt und an die Sozialversicherungsträger.

> Zulässig,

weil das Steuer- und Sozialversicherungsrecht das Unternehmen hierzu verpflichtet.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Arzt gibt die Adressdaten seiner Patienten an einen Arzneimittelhersteller weiter, damit dieser gezielt seine Medikamente bewerben kann.

> Unzulässig,

wenn das Arztmerkmal im Strafgesetzbuch die Weitergabe verbietet.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen regelt in einer Betriebsvereinbarung die Erhebung der Arbeitszeit und die Nutzung der anfallenden Daten zur Abrechnung von Gehalt, Urlaub und Überstunden.

> Zulässig,

weil nach der DS-GVO die **Beschäftigten** in der Verarbeitung durch eine Betriebsvereinbarung geregelt werden kann.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen veröffentlicht das Foto eines Vertriebsmitarbeiters auf seiner Internetseite.

> Zulässig,


wenn der Mitarbeiter zuvor in die Veröffentlichung eingewilligt hat.

DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT DATAKONTEXT

Ein Unternehmen beabsichtigt, seine Kunden (Verbraucher) Telefonisch auf seine neuen Produkte hinzuweisen.


> **Nur Zulässig**, wenn der Kunde seine Einwilligung in die Telefonwerbung gegeben hat.

DAS GANZE UNTERNEHMEN IST VERANTWORTLICH!



GESCHÄFTSFÜHRUNG
trägt die Verantwortung
für den Datenschutz nach
innen und nach außen

Delegiert einen Teil der
Verantwortung an die
Führungskräfte



FÜHRUNGSKRAFT
setzt gesetzliche und
interne betriebliche Rege-
lungen zum Datenschutz
um und kontrolliert deren
Einhaltung

Einschaltung vor Ein-
führung oder Änderung
datenschutzrelevanter
Geschäftsprozesse

Information bei Kenntnis
von Missbrauch, Verlust
oder Manipulation

Erteilung von Arbeitsanweisungen
und Befugnissen, Unterstützung bei
der Durchführung und Sensibilisie-
rung für die Bedeutung des Daten-
schutzes



DATENSCHUTZ-
BEAUFTRAGTER



MITARBEITER
schützt personenbezogene
Daten vor unbefugtem
Zugriff und unzulässiger
Weitergabe

Selbstkontrolle durch den Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte hat die Aufgabe, die Einhaltung des Datenschutzrechts zu überwachen. Er berät die Geschäftsführung und die Mitarbeiter und steht bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten zur Verfügung. Er unterliegt der Verschwiegenheitspflicht und hat das Recht, sich an die Datenschutz-Aufsichtsbehörde zu wenden.

In Unternehmen mit mindestens 20 Personen, die personenbezogene Daten automatisiert verarbeiten, muss ein Datenschutzbeauftragter bestellt werden. Wenn kein Datenschutzbeauftragter zu bestellen ist, nimmt weitgehend die Geschäftsführung dessen Aufgaben wahr.

Gibt es im Unternehmen eine Mitarbeitervertretung, kontrolliert auch diese die Einhaltung des Datenschutzes im Hinblick auf Mitarbeiterdaten.

BEI FRAGEN

zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wenden Sie sich bitte an Ihren betrieblichen Beauftragten für den Datenschutz.

2. Integrität

Weitergabekontrolle
 Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Art. 25 DS-GVO
 §
 fordert Datenschutz durch Technikgestaltung (privacy by design) und datenschutzfreundliche Voreinstellung (privacy by default).

- **Eingabekontrolle**
 Feststellung ob und wann fremdpersonbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentierung im IT

3. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**
 Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline, onsite/offsite), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

- **Rasche Wiederherstellbarkeit**

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

Auftragskontrolle

Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberprüfungspflicht, Nachkontrollen

DIE RECHTE DER BETROFFENEN PERSON

Diejenige natürliche Person, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekt des Gesetzes sind, bezeichnet das BDSG oder die DS-GVO als „betroffene Person“. Betroffene Personen können beispielsweise der Mitarbeiter, der Kunde oder der Ansprechpartner eines Firmenkunden sein. Den betroffenen Personen räumt die DS-GVO Transparenz- und Interventionsrechte ein.

INTERVENTIONSRECHTE

Die betroffene Person soll wissen, für welche Zwecke ihre Daten verarbeitet werden und welche Datenschutzrechte sie hat. Dies löst Transparenzpflichten beim Unternehmen aus.



ACHTUNG

Die betroffene Person kann sich mit Beschwerden oder Anfragen an den betrieblichen Datenschutzbeauftragten wenden. Dieser unterliegt hinsichtlich der betroffenen Person einer Verschwiegenheitsverpflichtung, sofern diese ihn nicht davon befreit hat.

Berichtigung

Es dürfen nur zutreffende Daten verarbeitet werden. Sonst sind diese zu berichtigen.

Löschung

Nach Zweckverbrauch oder dem Ablauf von Aufbewahrungsvorschriften sind Daten zu löschen.

Recht auf Vergessenwerden

Wenn das Unternehmen löschpflichtige Daten veröffentlicht hat, hat auf Verlangen der betroffenen Person das Unternehmen zu recherchieren, wer auf diese Daten verlinkt oder diese adaptiert hat. Diese Dritten sind über das Löschverlangen zu informieren.

BETROFFENE PERSON

**Einschränkung der Verarbeitung**

Wenn die Richtigkeit der Daten von betroffenen Personen bestritten wird oder die betroffene Person bei Löschpflicht die Daten zur Rechtsverfolgung benötigt, sind diese zu sperren. Dasselbe gilt für gesetzliche Aufbewahrungspflichten des Unternehmens.

Widerspruch

Die betroffene Person kann, aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Datenverarbeitung erheben, wenn deren Zulässigkeit auf einer Interessenabwägung beruht. Auch gegen Direktwerbung kann die betroffene Person Widerspruch einlegen.

Datenübertragung

Hat die betroffene Person Daten bereitgestellt, z.B. in einem sozialem Netzwerk oder einem Kundenkonto, sind diese Daten vom Verantwortlichen in einem gängigen, strukturierten maschinenlesbaren Format der betroffenen Person oder einem anderen Verantwortlichen zu übertragen.

FIT FÜR DEN DATENSCHUTZ? TESTEN SIE IHR WISSEN!

(Mehrfachnennungen möglich)

- 1 Die DS-GVO schützt...
 - a) Unternehmen.....
 - b) natürliche Personen.....
- 2 Die Datenschutzaufsichtsbehörde kann...
 - a) Mitarbeiter kündigen.....
 - b) Bußgelder verhängen.....
- 3 Die Verantwortung für den Datenschutz in Unternehmen hat...
 - a) jedes Mitarbeiter/Praktikant.....
 - b) die Führungskraft.....
 - c) der Mitarbeiter.....
- 4 Die Nutzung von eigenen Kundendaten zu Werbezwecken für einen Produkt ist grundsätzlich...
 - a) zulässig.....
 - b) unzulässig.....
- 5 Daten, die nicht mehr benötigt werden, sind...
 - a) zu löschen.....
 - b) einzuschränken.....
- 6 Die Zugangskontrolle kann unter anderem erreicht werden durch...
 - a) Abschließen von Räumen.....
 - b) Passwortschutz.....
- 7 Die Datenschutzkontrolle wird...
 - a) durchgeführt.....
 - b) durch die Aufsichtsbehörde.....
 - c) den betrieblichen Datenschutzbeauftragten.....
- 8 Falls ein Kunde keine Einwilligung wünscht, kann er verlangen, die Daten dafür...
 - a) zu löschen.....
 - b) einzuschränken.....
- 9 Die Verpflichtung zur Wahrung des Datengeheimnisses verlangt...
 - a) das Unterlassen unbefugter Datenverarbeitung.....
 - b) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses.....

PRAXISTIPPS ZUM DATENSCHUTZ

Jeder Mitarbeiter ist für den Datenschutz im Unternehmen mitverantwortlich. Nicht zuletzt im eigenen Interesse gehört zu seinen Aufgaben, sich an die Datenschutzregeln seines Unternehmens zu halten und seine Aufgaben mit Bedacht zum Datenschutz wahrzunehmen.

Einfache Datenschutztipps sind jedoch allgemeingültig:

Clean Desk



Ein aufgeräumter Schreibtisch, das Clean-Desk-Prinzip, sorgt für Datensicherheit und Vertraulichkeit. Personenbezogene Daten und Firmendokumente sind geschützt und gelangen nicht in die Hände Unbefugter. Bei Abwesenheit sollten Unterlagen, USB-Sticks, Datenträger etc. eingeschlossen sein.

Auskünfte am Telefon



Personenbezogene Auskünfte, sowohl intern als auch extern, sind mit Blick auf den Datenschutz kritisch zu prüfen. Insbesondere bei Auskünfteverträgen am Telefon ist mit Blick auf die Person des Anrufenden und den Inhalt ein Vorsicht geboten und im Zweifel auf den schriftlichen Weg zu verweisen.

Abmeldung am System



Bei längerer Abwesenheit vom Arbeitsplatz sollte man sich vom System abmelden.

Sichtschutz am Bildschirm



Der Bildschirm ist so zu positionieren, dass er vor dem unbefugten Einblick durch Kollegen, Besucher oder Kunden geschützt ist. Auf Reisen hilft ein sogenannter Blickschutzfilter.

Sichere Übermittlung von E-Mails



Wenn vertrauliche E-Mails sicher übermittelt werden sollen, müssen sie verschlüsselt sein. Erkundigen Sie sich bei Ihrer IT-Sicherheits- oder Datenschutzabteilung nach geeigneten Verschlüsselungsverfahren.

Öffnen von E-Mails



Die meisten Computerviren werden über E-Mail-Anhänge verbreitet. Diese enthalten Malware wie Viren, Trojanern oder Würmer. Falls der Virenschutz versagt, sollten Sie sich bei verdächtigen E-Mails immer durch Rücksprache vergewissern, dass der Anhang tatsächlich von der Person oder Institution verschickt wurde, die als Absender angegeben ist.

MERKE:

Datenschutz schützt Ihre Kollegen, Kunden und Sie selbst!

Bibliographische Informationen der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter <http://dnb.ddb.de> abrufbar.

Mitarbeiterinformation Datenschutz - Merkblatt für Mitarbeiter nach DS-GVO und BDSG

978-3-89577-872-8

GDD - Gesellschaft für Datenschutz und Datensicherheit e.V.

29. aktualisierte und korrigierte Auflage

© 2020 DATAKONTEXT GmbH, Frechen

www.datakontext.com

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Lizenzausgaben sind nach Vereinbarung möglich.

Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn

Gestaltung und Satz: Esther Constalla, Erdgeschoss Grafik, Hamburg

Illustration: Line Wittenmann, Artiserie, Münster

Grafische Überarbeitung: Matthias Lück, CreaTechs, Boppard

Bildnachweis (Cover): fizkes@fotolia.com

Printed in Germany

Für dieses Merkblatt werden Staffelpreise angeboten.

Informationen unter: 02234/98949-26

Hinweis: Aus Gründen der Lesbarkeit wird auf die Aneinanderreihung von männlichen und weiblichen Personenbezeichnungen verzichtet und stattdessen jeweils nur eine Form verwendet. Selbstverständlich richten sich alle Ausführungen gleichermaßen an Mitarbeiterinnen und Mitarbeiter.

MUSTER



Gesellschaft für Datenschutz
und Datensicherheit e.V.



DATAKONTEXT