



Merkblatt Datenschutz

Information für Beschäftigte zu DS-GVO und BDSG



WAS IST ...
DATENSCHUTZ?



Liebe Kolleginnen und Kollegen,

das Thema Datenschutz betrifft Sie in zweifacher Hinsicht. Zum einen als Kunden oder Beschäftigte, deren 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 Beschäftigten, 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 das 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 Information für Beschäftigte soll Ihnen einen Überblick über die Grundlagen des Datenschutzes geben und Sie über Ihre Rechte und Pflichten aufklären.

In meiner Funktion als Datenschutzbeauftragte/r stehe ich Ihnen selbstverständlich in allen Zweifelsfragen zur Verfügung. Bitte wenden Sie sich vertrauensvoll an mich.

Ihr/e Datenschutzbeauftragte/r

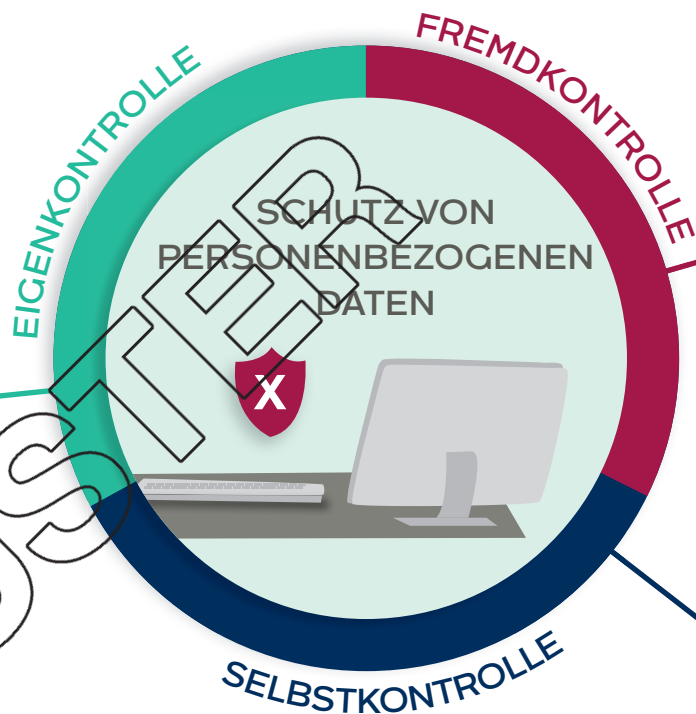
DATENSCHUTZ IM ÜBERBLICK

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 beanstanden, Bußgelder verhängen und Strafanträge stellen.

» **AB SEITE 6**



Das Unternehmen

... hat die Verantwortung

dafür, dass die Verarbeitung personenbezogener Daten nur entsprechend dem Datenschutzrecht erfolgt.

» **AB SEITE 8**

... organisiert den Datenschutz

Das Unternehmen macht die Vorgaben, wie und unter welchen Voraussetzungen personenbezogene 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?



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

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

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.

Was sind personenbezogene Daten?

Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimm- bare natürliche Person.

Beispiele

ADRESSE
GEBURTSDATUM
TELEFONNUMMER

VERMÖGEN
BESITZ
GEHALT
FOTO



ARBEITSVERHALTEN
PERSONALNUMMER
ARBEITSERGEBNISSE



BENUTZERKENNUNG
MASCHINENBEZOGENE
NUTZUNGSZEITEN

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 Verwendung ihrer personenbezogenen Daten. Geschützt sind demnach Beschäftigte, Kunden und Lieferanten oder deren Auftragspartner. (Lehmann, 2016, S. 10) Der Schutzbedarf von Daten hängt von ihrem Verwendungszusammenhang ab.

WER MUSS DIE

DS-GVO BEACHTEN?

1. 2. 3.

1. Privatrechtliche Organisationen und Firmen, aber auch Personen, die personensorientierte Daten verarbeiten, z.B. Selbstständige, Vereine, Produktions-, Handels- und Dienstleistungsbetriebe, aber auch Anbieter sozialer Netzwerke.

2. Sonstige privatwirtschaftliche Organisationen, deren Geschäftszweck die Verarbeitung personenbezogener Daten für fremde Zwecke ist wie Service-Recruiting-Agenturen, Wirtschaftsauskunfteien, Markt- und Meinungsforscher, Adressenhandler, -broker, und -verlage sowie wissenschaftliche Forschungseinrichtungen und Medien.

3. Öffentliche Stellen des Bundes und der Länder, z.B. die Bundesbehörden oder die Kommunalverwaltungen.

TEXT DATAKONTEXT DATAKONTEXT DATAKONTE

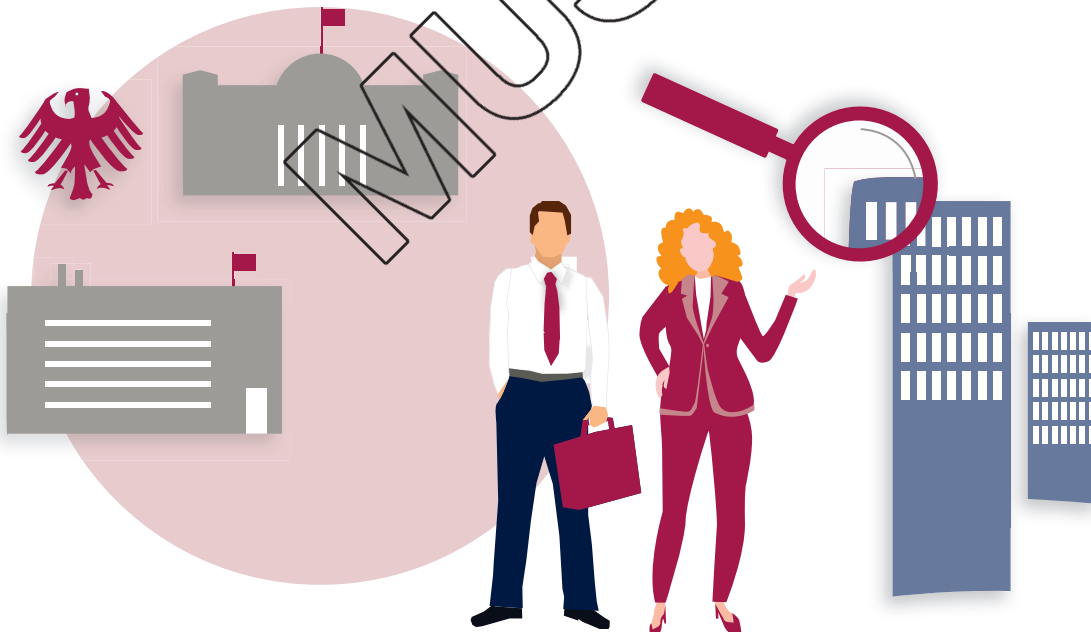
KONTROLLE DURCH DEN STAAT

DATAKONTEXT DATAK
Datenschutz-Aufsichtsbehörden

Die Aufsichtsbehörde kontrolliert die Datenschutzansätze 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-, Berichterstattungs-, Prüfungs- und Einsichtsrechte. Zudem kann die Aufsichtsbehörde erhebliche Bußgelder verhängen und Strafantrag stellen.

Die europäischen Aufsichtsbehörden stimmen sich in einem Datenschutzausschuss über die einheitliche Anwendung der DSGVO ab.

DATAKONTEXT DATAK
ONTEXT DATAKONTEXT



KONSEQUENZEN FÜR DAS UNTERNEHMEN

Ordnungswidrigkeiten sind vorsätzliche oder fahrlässige Datenschutzverstöße eines Unternehmens. Die Bußgeldandrohung ist massiv und beträgt bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten (Konzern-) Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Schadensersatzpflichten für das Unternehmen entstehen, wenn eine betroffene Person durch unzulässige oder unrichtige Datenhebung, Verarbeitung oder Nutzung einen Schaden erleidet. Das kann auch ein immaterieller Schaden sein. Das Unternehmen kann sich nur exculpieren, wenn es durch den Dienstleistungsaufweise die Verantwortung nicht verantwortlich zu sein. Das Unternehmen und sein Dienstleister sind für spätere Verarbeitungsläufen haftungsgesamtschuldnerisch.

Art. 83 DSGVO sieht Bußgelder von 20.000.000 Euro oder vier Prozent des weltweit erzielten Jahresumsatzes eines Unternehmens oder Konzerns bevorzähliger Datenverarbeitung oder Verstößen gegen die Betroffenenrechte. Bei Online-Angeboten können das Bußgeld 10.000.000 Euro oder zwei Prozent des weltweit erzielten Jahresumsatzes betragen.

Eine große Gefahr

Für das Unternehmen sind Reputations- und Imageschäden!

FÜR DIE BESCHÄFTIGTEN

Straftaten

sind vorsätzliche Handlungen des Beschäftigten durch rechtswidrige Datenverarbeitungen, die gegen Entgelt oder in Schädigungs- oder Bereicherungsbegabe gehen werden. Antragsberechtigt ist nicht nur der Betroffene, sondern auch die Datenschutz-Aufsichtsbehörde und das Unternehmen.

Schadensersatzpflichten

entstehen unter Umständen auch für den verantwortlichen Beschäftigten gegenüber seinem Arbeitgeber, wenn er sich nicht an seine Pflichten zur Beachtung des Datenschutzes gehalten hat.

Arbeitsrechtliche Konsequenzen

Verstöße gegen den Datenschutz können für den Beschäftigten auch arbeitsrechtliche Konsequenzen von der Abmahnung bis zur Kündigung haben.

Strafrechtlich relevant Verstöße gegen den Datenschutz werden mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

DIE VERANTWORTUNG DES UNTERNEHMENS

Das Unternehmen hat die Verantwortung für den Datenschutz. Die DSGVO spricht das Selbst von Verantwortlichen. Die meisten, die lediglich Datenverarbeitung im Auftrag betreiben (z.B. Service-Rechenzentren, Entsorger) werden der verantwortlichen Stelle zugeordnet.

Wann müssen Unternehmen die DS-GVO beachten?

Art. 5 DS-GVO

Grundsätze der Verarbeitung von personenbezogener Daten

- ▶ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- ▶ Zweckbindung
- ▶ Datenminimierung
- ▶ Richtigkeit
- ▶ Speicherungsdauer begrenzt
- ▶ Integrität und Vertraulichkeit

Die DS-GVO und das BDSG greifen überall dort, wo personenbezogene Daten verarbeitet werden, sei es mittels IT oder in strukturierten Datensammlungen wie z.B. Karteikarten oder Adressen. Daten für die Daten von Beschäftigten genauso wie die von Kunden oder Lieferanten. Die Zulässigkeit der Verarbeitung von Beschäftigten-Daten ist nicht auf Daten beschränkt. Jede Information über einen Beschäftigten muss datenschutzkonform erlangt und erfasst werden.

Datenschutzmaßnahmen

Die DS-GVO fordert von Unternehmen in Abhängigkeit vom Risiko für die betroffenen Person von Datenmissbrauch angemessene Technische und Organisatorische Maßnahmen müssen umgesetzt, regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Beachtung der Grundsätze der Datenverarbeitung und das Datenschutzmanagement müssen von Unternehmen nachgewiesen werden.

Wem 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 Beauftragte der Fachbereiche verantwortlich. Sie müssen die rechtlichen Vorgaben und Regelungen der Unternehmens umsetzen. Deshalb sollen diese Personen mit der Datenverarbeitung betrauten Personen über die Vorschriften der DS-GVO und des BDSG und gegebenenfalls über weitere relevante Datenschutzvorschriften informieren. Zudem sollten sie von Beginn ihrer Tätigkeit auf das Unternehmen im verpflichtet werden.

Für Beschäftigte von Dienstleistern der Auftragsdatenverarbeitung 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.

DS-GVO



oder

BDSG



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 Verarbeitung besonders sensibler Daten, z.B. Gesundheit, Religion oder Biometrie
- zur Datenübermittlung an Auskunftsteien
- 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 PERSONEN-BEZOGENEN 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).

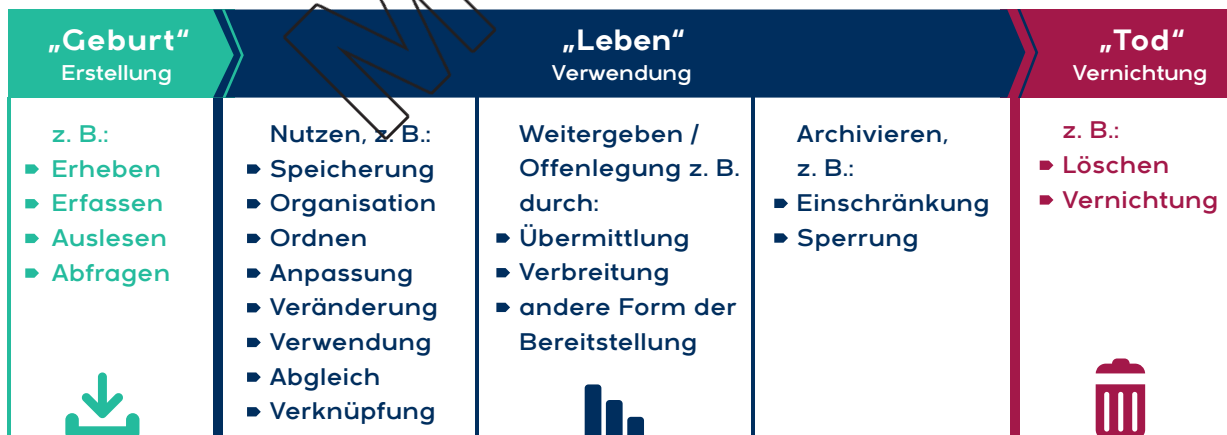
Der Begriff der Verarbeitung im Sinne der DS-GVO erfasst jeden Vorgang des Umgangs mit personenbezogenen Daten. Die Verarbeitung beginnt bei der Datenbeschaffung beim Betroffenen (z.B. durch schriftliche oder mündliche Befragung) oder bei Dritten (z.B. Kauf von Adressen bei einem Adresshändler) und reicht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



MERKSATZ

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

DATA-LIFE-CYCLE



BEISPIELE: ZULÄSSIG ODER NICHT?

Ein Unternehmen speichert seine Kundendaten zur Abwicklung eines Kaufvertrages und zur Prüfung möglicher Gewährleistungsansprüche.	Zulässig,	weil die Datenverarbeitung auf Grund einer bestehenden Vertragsbeziehung erfolgt.
Ein Unternehmen verschickt Mailings per Post an seine Besten, den Kundenstamm, um ein neu eingeführtes Produkt zu bewerben.	Zulässig,	weil Kundendaten auch für Zwecke der Werbung verwendet werden dürfen.
Auswertung von Daten für eigene Werbeziele, obwohl der Kunde erklärt hat, keine Werbung erhalten zu wollen.	Unzulässig,	wenn bei einem Werbeversuch die Daten für diesen Zweck nicht genutzt werden dürfen.
Ein Unternehmen übermittelt die Lohn- und Einkommensdaten seiner Beschäftigten an das Finanzamt und an die Sozialversicherungsträger.	Zulässig,	weil das Steuer- und Sozialversicherungsrecht das Unternehmen hierzu verpflichtet.
Ein Arzt gibt die Adressdaten seiner Patienten an einen Arzneimittelhersteller weiter, damit dieser gezielt seine Medikamente bewerben kann.	Unzulässig,	weil das Arztgeheimnis im Strafgesetzbuch die Weitergabe verbietet.
Ein Unternehmen regelt in einer Betriebsvereinbarung die Erfassung der Arbeitszeit und die Nutzung der anfallenden Daten zum Abrechnen von Gehältern, Urlaub und Überstunden.	Zulässig,	weil nach der DS-GVO die Beschäftigten datenverarbeitung durch eine Betriebsvereinbarung geregelt werden kann.
Ein Unternehmen veröffentlicht das Foto eines Vertriebsmitarbeiters auf seiner Internetseite.	Zulässig,	wenn der Mitarbeiter zuvor in die Veröffentlichung eingewilligt hat.
Beschäftigte geben personenbezogene Daten von anderen Beschäftigten und Kunden in das KI-System ChatGPT ein.	Unzulässig,	solange die Nutzung in diesem KI-System ungeklärt ist.

DAS GANZE UNTERNEHMEN IST VERANTWORTLICH!

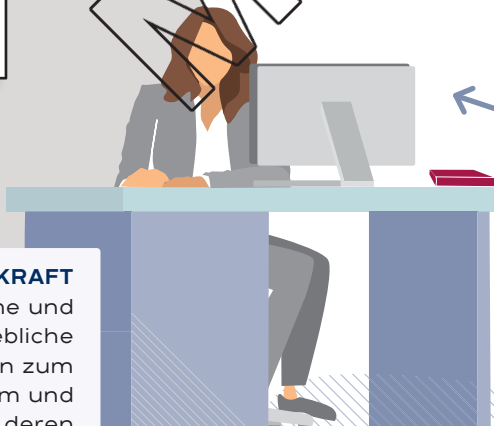


GESCHÄFTSFÜHRUNG
trägt die Verantwortung für den Datenschutz nach innen und nach außen

Delegiert einen Teil der Verantwortung an die Führungskräfte



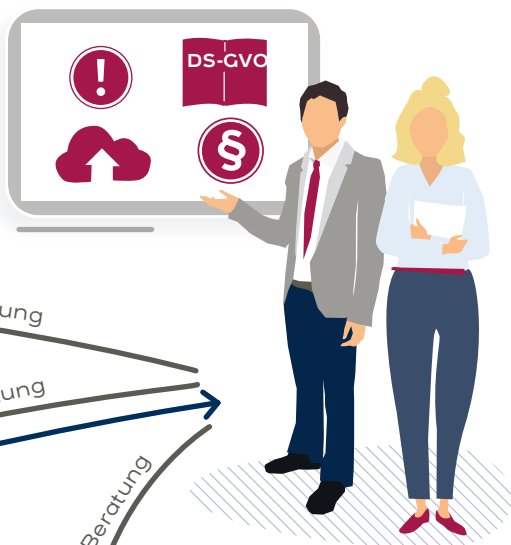
Einschaltung vor Einführung oder Änderung datenschutzrelevanter Geschäftsprozesse



FÜHRUNGSKRAFT
setzt gesetzliche und interne betriebliche Regelungen zum Datenschutz um und kontrolliert deren Einhaltung

Erteilung von Arbeitsanweisungen und Befugnissen, Unterstützung bei der Durchführung und Sensibilisierung für die Bedeutung des Datenschutzes

Information bei Kenntnis von Missbrauch, Verlust oder Manipulation



Beratung

Beratung

Beratung

**DATENSCHUTZ-
BEAUFTRAGTE**

Selbstkontrolle durch Datenschutzbeauftragte

Betriebliche Datenschutzbeauftragte haben die Aufgabe, die Einhaltung des Datenschutzrechts zu überwachen. Sie beraten die Geschäftsführung und die Beschäftigten und stehen bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten zur Verfügung. Sie unterliegen der Verschwiegenheitspflicht und haben das Recht, sich an die Datenschutz-Aufsichtsbehörde zu wenden.

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

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



BESCHÄFTIGTE

schützen personen-
bezogene Daten vor
unbefugtem Zugriff und
unzulässiger Weitergabe

BEI FRAGEN

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

SICHERHEITZIELE ZUR DATENSICHERHEIT



Art. 3 DS-GVO fordert ein Datensicherheitsmanagement mit geeigneten technischen und organisatorischen Maßnahmen

Zur Aufrechterhaltung der Sicherheit und zur Vermeidung von Datenschutzverstößen hat das Unternehmen die mit der Verarbeitung verbundene Risiken zu ermitteln und Maßnahmen zu ihrer Eindämmung zu treffen. Folgende Ziele sind zu erreichen:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

1. Vertraulichkeit

• Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Videoüberwachungszwischenräume, Alarmanlagen, Videoanlagen

• Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

• Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen in der Hardware des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

• Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Manpowerfähigkeiten

• Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzufügung zusätzlicher Informationen nicht einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

2. Integrität

■ Weitergabekontrolle

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

■ Eingabekontrolle

Festschaltung, Auswahl von Weitergabepersonenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

3. Verfügbarkeit und Belastbarkeit

■ Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-, Strategie (online/offline, on-site/off-site), Unterbrechungsfreie Stromversorgung (USV), Viruschutz, Firewall, Meldewege und Notfallpläne

■ Risiko- und Wiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

■ Datenschutz-Management

■ Incident-Response-Management

■ Datenschutzrechtliche Vereinbarungen (Art. 25 Abs. 2 DS-GVO)

■ Auftragskontrolle

Keine Auftragdatenverarbeitung ohne entsprechende Vereinbarung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorüberzeugungs-pflicht, Nachkontrollen

Art. 5 DS-GVO

fordert Datenschutz durch Technikgestaltung (privacy by design) und datenschutzfreundliche Voreinstellung (privacy by default).



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 Beschäftigte, der Kunde oder Kundin oder auch 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 betriebliche Datenschutzbeauftragte wenden. Diese unterliegen hinsichtlich der betroffenen Person einer Verschwiegenheitsverpflichtung, sofern diese sie 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.

TRANSPARENZPFLICHTEN DES UNTERNEHMENS

DATAKONTEXT DATAKONTEXT D
ATAKONTEXT DATAKONTEXT DA
TAKONTEXT DATAKONTEXT DAT
AKONTEXT DATAKONTEXT DATA
KONTEXT DATAKONTEXT DATAK
ONTEXT DATAKONTEXT DATAKO
NTEXT DATAKONTEXT DATAKON
TEXT DATAKONTEXT DATAKONT
EXT DATAKONTEXT DATAKONTE
XT DATAKONTEXT DATAKONTEXT
T DATAKONTEXT DATAKONTEXT
DATAKONTEXT DATAKONTEXT D



Informationspflichten

Bereits bei der Datenerhebung muss das Unternehmen die betroffene Person über ihre Identität, alle Zweckbestimmungen der Datenverarbeitung sowie mögliche Kategorien von Empfängern und um Speicherdauer informieren. Zugleich ist sie über die Kontaktmöglichkeit zum Datenschutzbeauftragten sowie über ihre Rechte zu informieren.

Benachrichtigung

Wenn Daten über die betroffene Person von Dritten oder aus öffentlichen Quellen erhoben worden sind, ist die betroffene Person auf dem gleichen Informationsstand zu bringen, als wenn Daten über ihr erhoben worden wären.

Auskunft

Falls die betroffene Person anfragt, ist die verantwortliche Stelle zur Auskunft über die gespeicherten Daten, deren Herkunft und mögliche Empfänger, sowie über den Zweck der Speicherung verpflichtet. Weiterhin ist die betroffene Person über ihre Betroffenenrechte zu informieren. Die Auskunft ist unverzüglich zu erteilen.

FIT FÜR DEN DATENSCHUTZ? TESTEN SIE IHR WISSEN!

(Mehrfachnennungen möglich)

1. Die DS-GS schützt ...
 - a) Unternehmen
 - b) natürliche Personen
 - c) Beschäftigte und ihre Familienangehörige
 - d) alle natürlichen Personen
2. Die Datenschutzaufsicht beschließen kann ...
 - a) Bußgelder verhängen
 - b) die Geschäftsführung/Vorstand
 - c) die Führungskraft
 - d) die Beschäftigten
3. Die Verantwortung für den Datenschutz im Unternehmen hat ...
 - a) die Geschäftsführung/Vorstand
 - b) die Führungskraft
 - c) die Beschäftigten
 - d) die Aufsichtsbehörde
4. Die Nutzung von eigenen Kundendaten zu Werbezwecken für eigene Produkte ist grundsätzlich ...
 - a) zulässig
 - b) unzulässig
 - c) zulässig, wenn die Kunden zuvor informiert wurden
 - d) unzulässig, wenn die Kunden zuvor informiert wurden
5. Daten, die nicht mehr benötigt werden, sind ...
 - a) zu löschen
 - b) einzuschränken
 - c) zu archivieren
 - d) zu veröffentlichen
6. Die Zugangskontrolle kann unter anderem erreicht werden durch ...
 - a) Abschließen von Türen
 - b) Passwortschutz
 - c) die Beschäftigtenvertretung
 - d) die Aufsichtsbehörde
7. Die Datenschutzkontrolle wird ausgeübt durch ...
 - a) die Beschäftigtenvertretung
 - b) die Aufsichtsbehörde
 - c) die betrieblichen Datenschutzbeauftragten
 - d) die Betriebsrat
8. Falls ein Kunde eine Löschung wünscht kann er verlangen, die Daten dafür ...
 - a) zu löschen
 - b) einzuschränken
 - c) zu archivieren
 - d) zu veröffentlichen
9. Die Verpflichtung zur Wahrung des Dateneigentums verlangt ...
 - a) das Unterlassen ungelegter Datenvorbereitung
 - b) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses
 - c) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses
 - d) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses

PRAXISTIPPS ZUM DATENSCHUTZ

Jeder Beschäftigte 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 Bezug 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 Firmengeheimnisse sind geschützt und gelangen nicht in die Hände Unberechtigter. Bei Abwesenheit sollten Unterlagen, USB-Sticks, Datenträger etc. eingeschlossen sein.

Auskünfte am Telefon oder per Mail

Personenbezogene Auskünfte, ob vom Internetauftritt, Telefonat oder mit Blick auf den Datenschutz kritisch zu prüfen. Insbesondere bei Auskunftsverlangen am Telefon oder per Mail ist mit Blick auf die Art sowie den Inhalt der Auskunft abzuheben und im Zweifelsfall der Schriftweg zu bevorzugen.

Abmeldung am System

Bei Abwesenheit vom Arbeitsplatz sollte man sich vom System abmelden.

Sichtschutz am Bildschirm

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

Sichere Übermittlung von E-Mails

Wenn vertrauliche E-Mails sicher übermitteln werden sollen, müssen sie verschlüsselt sein. Erkundigen Sie sich bei Ihren IT-Sicherheits- oder Datenschutzbeauftragten nach geeigneten Verfahrenslösungen.

Öffnen von E-Mail

Die meisten Computerviren werden über E-Mailanhänge verbreitet. Diese enthalten Malware wie Viren, Trojaner oder Würmer. Falls eine Viruswarnung ertönt, sollten Sie sich bei Verdähten E-Mails immer durch Rücksprache vergewissern, dass der Anhang tatsächlich von der Person oder Institution geschickt wurde, die als Absender angegeben ist.

Besondere Vorsicht und Schutzmaßnahmen beim Homeoffice und mobilen Arbeiten.

» MERKE:

Datenschutz schützt Ihre Kollegen und Kolleginnen, 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.

Merkblatt Datenschutz - Information für Beschäftigte zu DS-GVO und BDSG

ISBN 978-3-98746-005-0

GDD - Gesellschaft für Datenschutz und Datensicherheit e.V.

30. überarbeitete und aktualisierte Auflage

© 2024 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. Lizenzangaben sind nach Vereinbarung möglich.

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

Gestaltung: Esther Gonstalla, Erdgeschoss Grafik, Angelsee

Illustration: Line Wittemann, Artiserie, Münster

Satz: Matthias Lück, CreaTechs, Boppard

Bildnachweis (Cover): fizkes © www.fotolia.de

Hersteller: DATAKONTEXT GmbH, Augustinusstr. 11A, 50226 Frechen

Kontakt und Informationen zum Thema Produktsicherheitsverordnung:

Per Telefon: 02234 9894999

Per Mail: dieter.schulz@datakontext.com

<https://www.datakontext.com/produktsicherheitsverordnung>

Printed in Germany

Für dieses Merkblatt werden Staffelpreise angeboten.

Informationen unter: 02234/98949-30

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

MUSTER

GDD

Gesellschaft für Datenschutz
und Datensicherheit e.V.



DATAKONTEXT

