

Datenschutz - DSGVO und BDSG

Datenschutz - DSGVO und BDSG

Datenschutz schützt Menschen beim Umgang mit ihren personenbezogenen Daten.

Er legt fest, welche Daten erhoben werden dürfen, wofür sie verwendet werden dürfen und welche Rechte die betroffenen Personen haben.

Beispiel: Ein Unternehmen darf Kundenadressen zur Auslieferung einer Bestellung verwenden. Es darf die Daten aber nicht beliebig für andere Zwecke weitergeben.

Datenschutz und Datensicherheit unterscheiden

Begriff	Bedeutung	Beispiel
Datenschutz	Regelt den zulässigen Umgang mit personenbezogenen Daten	Wer darf Mitarbeiterdaten für welchen Zweck verwenden?
Datensicherheit	Schützt Daten vor Verlust, Manipulation und unbefugtem Zugriff	Verschlüsselung, Backups und Zugriffsrechte

Merksatz: Datenschutz fragt: „Darf ich die Daten verarbeiten?“ Datensicherheit fragt: „Wie schütze ich die Daten?“

Übungsfrage: Was unterscheidet Datenschutz und Datensicherheit?

Musterantwort: Datenschutz schützt Menschen bei der Verarbeitung ihrer personenbezogenen Daten. Datensicherheit schützt alle Arten von Daten vor Verlust, Veränderung und unberechtigttem Zugriff.

DSGVO - Datenschutz-Grundverordnung

Die DSGVO ist eine Verordnung der Europäischen Union. Sie gilt seit dem **25. Mai 2018** unmittelbar in allen EU-Mitgliedstaaten.

Sie regelt insbesondere:

- den Umgang mit personenbezogenen Daten,
- die Rechte betroffener Personen,
- die Pflichten von Unternehmen, Behörden und anderen verantwortlichen Stellen.

Was bedeutet Datenverarbeitung?

Zur Verarbeitung gehören beispielsweise:

- Daten erheben,
- Daten speichern,
- Daten auslesen und verwenden,
- Daten verändern,
- Daten weitergeben,
- Daten löschen.

Beispiel: Ein Unternehmen erfasst die Adresse eines Kunden, speichert sie im Bestellsystem und übermittelt sie an einen Versanddienstleister. Alle diese Schritte sind Datenverarbeitungen.

Wann dürfen personenbezogene Daten verarbeitet werden?

Eine Verarbeitung benötigt eine Rechtsgrundlage. Häufige Beispiele sind:

Rechtsgrundlage	Einfaches Beispiel
Einwilligung	Eine Person stimmt dem Erhalt eines Newsletters zu.
Vertragserfüllung	Ein Onlineshop benötigt die Lieferadresse, um die bestellte Ware zu versenden.
Gesetzliche Verpflichtung	Ein Unternehmen bewahrt bestimmte Rechnungsdaten aufgrund gesetzlicher Vorgaben auf.
Berechtigtes Interesse	Bestimmte Sicherheitsprotokolle können zum Schutz eines IT-Systems erforderlich sein. Dabei müssen die Interessen der Betroffenen berücksichtigt werden.

Daneben gibt es weitere Rechtsgrundlagen, beispielsweise für öffentliche Aufgaben oder zum Schutz lebenswichtiger Interessen.

Wichtig: Eine Einwilligung ist nicht für jede Datenverarbeitung erforderlich. Es kann auch eine andere passende Rechtsgrundlage vorliegen.

Anforderungen an eine Einwilligung

Eine Einwilligung muss:

- freiwillig sein,
- auf verständlichen Informationen beruhen,
- für einen bestimmten Zweck erfolgen,
- durch eine eindeutige Handlung erteilt werden.

Sie muss widerrufen werden können. Der Widerruf muss so einfach sein wie die Erteilung.

Beispiel: Ein freiwilliges, nicht vorausgewähltes Kästchen für einen Newsletter.

Übungsfrage: Wofür steht DSGVO und was regelt sie?

Musterantwort: DSGVO bedeutet Datenschutz-Grundverordnung. Sie regelt den Umgang mit personenbezogenen Daten sowie die Rechte der Betroffenen und die Pflichten der verantwortlichen Stellen.

Übungsfrage: Benötigt ein Onlineshop eine zusätzliche Einwilligung, um eine notwendige Lieferadresse für die Bestellung zu verarbeiten?

Musterantwort: Nein. Die erforderliche Verarbeitung kann auf der Vertragserfüllung beruhen. Die Adresse darf deshalb aber nicht automatisch für beliebige andere Zwecke genutzt werden.

Wichtige Grundprinzipien

Die DSGVO enthält Grundsätze für den Umgang mit personenbezogenen Daten.

Grundprinzip	Einfach erklärt	Beispiel und Umsetzung
Rechtmäßigkeit	Es muss eine passende Rechtsgrundlage geben.	Vor der Verarbeitung prüfen, ob beispielsweise ein Vertrag oder eine Einwilligung vorliegt.
Verarbeitung nach Treu und Glauben	Menschen dürfen bei der Verarbeitung nicht unfair behandelt oder getäuscht werden.	Ein Gewinnspiel darf nicht verschleiern, dass Daten für Werbung gesammelt werden sollen.
Transparenz	Die Verarbeitung muss verständlich erklärt werden.	Informationen über Zweck, Empfänger und Speicherdauer bereitstellen.
Zweckbindung	Daten werden für festgelegte Zwecke erhoben und dürfen nicht beliebig anders verwendet werden.	Eine Lieferadresse nicht ohne weitere Prüfung für eine andere Nutzung übernehmen.
Datenminimierung	Nur die notwendigen Daten verarbeiten.	Bei einer Newsletteranmeldung normalerweise keine Postanschrift verlangen.
Richtigkeit	Daten müssen sachlich richtig und bei Bedarf aktuell sein.	Eine gemeldete Adressänderung übernehmen.
Speicherbegrenzung	Daten nicht länger als erforderlich aufbewahren.	Löschfristen festlegen und nicht mehr benötigte Daten löschen.
Integrität und Vertraulichkeit	Daten gegen unzulässige Veränderung, Verlust und unbefugten Zugriff schützen.	Berechtigungen, Verschlüsselung und Datensicherungen einsetzen.

Rechenschaftspflicht

Das Unternehmen muss nachweisen können, dass es die Datenschutzgrundsätze einhält.

Beispiele:

- Einwilligungen dokumentieren.
- Zuständigkeiten festlegen.
- Löschregeln dokumentieren.
- Sicherheitsmaßnahmen und deren Prüfung nachweisen.

Wichtige Unterschiede

- **Datenminimierung:** Welche und wie viele Daten werden benötigt?
- **Zweckbindung:** Wofür werden die Daten verwendet?
- **Speicherbegrenzung:** Wie lange werden die Daten benötigt?

Wichtig: Gesetzliche Aufbewahrungspflichten können verhindern, dass bestimmte Daten sofort gelöscht werden dürfen.

Übungsfrage: Ein Newsletterformular verlangt zusätzlich die Schuhgröße. Welcher Grundsatz ist betroffen?

Musterantwort: Die Datenminimierung. Für einen gewöhnlichen Newsletter wird die Schuhgröße nicht benötigt.

Übungsfrage: Ein Unternehmen speichert nicht mehr benötigte Kundendaten ohne festgelegtes Ende. Welcher Grundsatz ist betroffen?

Musterantwort: Die Speicherbegrenzung. Das Unternehmen muss prüfen, wie lange die Daten erforderlich sind und ob Aufbewahrungspflichten bestehen.

Übungsfrage: Nennen Sie drei Maßnahmen zum Schutz personenbezogener Daten.

Musterantwort: Zugriffsrechte auf berechtigte Personen beschränken, Daten verschlüsseln und regelmäßige Backups erstellen.

BDSG - Bundesdatenschutzgesetz

Das BDSG ergänzt die DSGVO in Deutschland dort, wo nationale Regelungen vorgesehen sind.

Es enthält insbesondere Regelungen zu:

- bestimmten nationalen Datenschutzfragen,
- personenbezogenen Daten im Beschäftigungsverhältnis,
- Aufgaben und Befugnissen der Bundesdatenschutzaufsicht,
- zusätzlichen Anforderungen an die Benennung von Datenschutzbeauftragten.

Beispiel aus dem Beschäftigtenverhältnis

Ein Arbeitgeber verarbeitet die Bankverbindung seiner Beschäftigten, um das Gehalt auszuzahlen.

Die Daten dürfen nur für zulässige Zwecke verwendet werden. Nicht jeder Beschäftigte benötigt Zugriff darauf.

DSGVO und BDSG unterscheiden

DSGVO	BDSG
Europäische Verordnung	Deutsches Bundesgesetz
Enthält die grundlegenden Datenschutzregeln	Ergänzt diese durch nationale Regelungen
Gilt unmittelbar in allen EU-Mitgliedstaaten	Gilt in seinem Anwendungsbereich in Deutschland

Merksatz: Die DSGVO bildet die europäische Grundlage. Das BDSG ergänzt sie in Deutschland.

Übungsfrage: Ersetzt das BDSG die DSGVO?

Musterantwort: Nein. Das BDSG ergänzt die DSGVO durch nationale Regelungen.

Übungsfrage: Nennen Sie ein Beispiel für personenbezogene Daten im Beschäftigungsverhältnis.

Musterantwort: Die Bankverbindung eines Mitarbeiters für die Gehaltszahlung. Auch Personalnummer, Adresse und Arbeitszeitdaten sind mögliche Beispiele.

Personenbezogene Daten

Personenbezogene Daten sind Informationen, die sich auf einen bestimmten oder bestimmbaren Menschen beziehen.

Die Person muss nicht direkt mit ihrem Namen genannt werden. Es genügt, wenn sie mithilfe zusätzlicher Informationen identifiziert werden kann.

Beispiel	Warum personenbezogen?
Name	Bezeichnet eine Person.
Adresse	Kann einer Person zugeordnet werden.
Persönliche E-Mail-Adresse	Kann eine Person erkennbar machen.
IP-Adresse	Kann unter entsprechenden Umständen einer Person zugeordnet werden.

Beispiel	Warum personenbezogen?
Telefonnummer	Kann einer Person zugeordnet werden.
Personalnummer	Der Arbeitgeber kann sie einem Beschäftigten zuordnen.
Standortdaten	Können Aufenthaltsorte und Bewegungen einer Person erkennen lassen.

Wichtig: Auch eine geschäftliche E-Mail-Adresse wie „vorname.nachname@firma.de“ kann personenbezogen sein.

Besonders schützenswerte Daten

Für bestimmte Daten gelten strengere Regeln. Dazu gehören beispielsweise:

- Gesundheitsdaten,
- Angaben zur Religion,
- politische Meinungen,
- biometrische Daten zur eindeutigen Identifizierung.

Beispiel: Angaben über Erkrankungen eines Mitarbeiters dürfen nicht für alle Beschäftigten sichtbar sein.

Anonymisierung und Pseudonymisierung

Begriff	Bedeutung	Beispiel
Anonymisierung	Eine Person ist nicht mehr mit vernünftigerweise einsetzbaren Mitteln bestimmbar.	Eine ausreichend zusammengefasste Statistik ohne Rückschluss auf Einzelpersonen
Pseudonymisierung	Direkte Angaben werden ersetzt; mit Zusatzinformationen bleibt eine Zuordnung möglich.	Namen werden durch Kennnummern ersetzt, eine getrennte Liste enthält die Zuordnung.

Merksatz: Pseudonymisierte Daten bleiben personenbezogen. Wirklich anonymisierte Daten fallen nicht unter die DSGVO.

Übungsfrage: Nennen Sie vier personenbezogene Daten.

Musterantwort: Name, Adresse, persönliche E-Mail-Adresse und Telefonnummer.

Übungsfrage: Sind Personalnummern personenbezogene Daten?

Musterantwort: Ja. Der Arbeitgeber kann die Personalnummer einer bestimmten Person zuordnen.

Übungsfrage: Namen werden durch Nummern ersetzt. Eine Zuordnungsliste wird aufbewahrt. Sind die Daten anonymisiert?

Musterantwort: Nein. Sie sind pseudonymisiert, weil die Personen mithilfe der Zuordnungsliste weiterhin bestimmbar sind.

Rechte der betroffenen Personen

Betroffene Personen haben verschiedene Rechte gegenüber der verantwortlichen Stelle.

Recht	Einfach erklärt	Beispiel
Recht auf Information	Die Verarbeitung muss erklärt werden.	Ein Kontaktformular informiert über Zweck und Umgang mit den eingegebenen Daten.
Auskunftsrecht	Betroffene können erfahren, ob und welche Daten über sie verarbeitet werden.	Ein Kunde fragt nach seinen gespeicherten Daten und erhält die vorgesehenen Informationen sowie eine Datenkopie.
Berichtigungsrecht	Falsche Daten müssen korrigiert werden können.	Eine falsche Anschrift wird berichtigt.
Recht auf Löschung	Daten müssen unter bestimmten Voraussetzungen gelöscht werden.	Nicht mehr benötigte Profildaten werden entfernt.
Einschränkung der Verarbeitung	Daten dürfen unter bestimmten Voraussetzungen vorerst nur eingeschränkt genutzt werden.	Eine beanstandete Angabe wird während ihrer Überprüfung nicht regulär weiterverwendet.
Datenübertragbarkeit	Bestimmte bereitgestellte Daten können in einem gängigen, maschinenlesbaren Format verlangt werden.	Ein Nutzer erhält geeignete Daten als CSV-Datei für einen Anbieterwechsel.
Widerspruchsrecht	Gegen bestimmte Verarbeitungen kann widersprochen werden.	Eine Person widerspricht der Nutzung ihrer Daten für Direktwerbung.

Information und Auskunft unterscheiden

- **Information:** Die verantwortliche Stelle informiert grundsätzlich von sich aus über die Verarbeitung.
- **Auskunft:** Eine Person fragt gezielt nach der Verarbeitung ihrer eigenen Daten.

Löschung ist nicht immer sofort möglich

Eine Löschanfrage bedeutet nicht automatisch, dass sämtliche Daten sofort entfernt werden müssen.

Beispiel: Bestimmte Rechnungsdaten müssen möglicherweise aufgrund gesetzlicher Pflichten weiter aufbewahrt werden. Nicht mehr benötigte Profildaten können trotzdem zu löschen sein.

Datenübertragbarkeit gilt nicht für alle Daten

Sie betrifft insbesondere bereitgestellte Daten, die automatisiert auf Grundlage einer Einwilligung oder eines Vertrags verarbeitet werden.

Widerspruch gegen Werbung

Nach einem Widerspruch gegen Direktwerbung dürfen die personenbezogenen Daten nicht mehr für diesen Werbezweck verarbeitet werden.

Wichtige Frist

Über Maßnahmen zu Anträgen auf Betroffenenrechte muss grundsätzlich unverzüglich, spätestens innerhalb eines Monats informiert werden. In begründeten Fällen ist eine Verlängerung möglich; darüber muss innerhalb des ersten Monats informiert werden.

Praktische Umsetzung im Unternehmen

1. Anfrage an die zuständige Stelle weiterleiten.
2. Bei Bedarf die Identität angemessen prüfen.
3. Betroffene Daten und mögliche Ausnahmen prüfen.
4. Die erforderlichen Maßnahmen fristgerecht umsetzen.
5. Den Vorgang dokumentieren.

Übungsfrage: Ein Kunde möchte wissen, welche Daten über ihn gespeichert sind. Welches Recht nutzt er?

Musterantwort: Das Auskunftsrecht.

Übungsfrage: Ein Kunde meldet eine falsch gespeicherte Adresse. Welches Recht ist betroffen?

Musterantwort: Das Recht auf Berichtigung.

Übungsfrage: Müssen nach einer Löschanfrage sofort auch alle aufbewahrungspflichtigen Rechnungsdaten gelöscht werden?

Musterantwort: Nein. Gesetzliche Aufbewahrungspflichten können einer sofortigen Löschung entgegenstehen.

Übungsfrage: Eine Person möchte keine Direktwerbung mehr erhalten. Was muss das Unternehmen tun?

Musterantwort: Die Verarbeitung ihrer Daten für Direktwerbung einstellen und den Widerspruch berücksichtigen.

Pflichten von Unternehmen

Unternehmen müssen Datenschutz im Arbeitsalltag organisieren und umsetzen.

Pflicht	Einfache Umsetzung
Daten rechtmäßig verarbeiten	Rechtsgrundlage und Zweck vorab prüfen.
Betroffene informieren	Verständliche Datenschutzhinweise bereitstellen.
Daten angemessen schützen	Technische und organisatorische Maßnahmen einsetzen.
Betroffenenrechte ermöglichen	Zuständigkeiten für Auskunft, Berichtigung und Löschung festlegen.
Datenschutzverletzungen behandeln	Vorfälle dokumentieren, Risiken bewerten und gegebenenfalls melden.
Gegebenenfalls einen Datenschutzbeauftragten benennen	Prüfen, ob die gesetzlichen Voraussetzungen vorliegen.
Einhaltung nachweisen	Wichtige Entscheidungen, Verfahren und Maßnahmen dokumentieren.

Datenschutzhinweise

Sie erklären beispielsweise:

- Wer ist für die Verarbeitung verantwortlich?
- Welche Daten werden wofür verarbeitet?
- Auf welcher Rechtsgrundlage geschieht das?
- Wer erhält die Daten?
- Wie lange werden sie gespeichert?
- Welche Rechte haben die betroffenen Personen?

Wichtig: Eine Datenschutzerklärung allein macht eine unzulässige Datenverarbeitung nicht erlaubt.

Technische und organisatorische Maßnahmen

Technische Maßnahme	Beispiel
Zugriffsschutz	Persönliche Benutzerkonten und passende Berechtigungen
Verschlüsselung	Verschlüsseltes Notebook und sichere Datenübertragung

Technische Maßnahme	Beispiel
Datensicherung	Regelmäßige Backups mit Wiederherstellungstests
Schutz des Arbeitsplatzes	Automatische Bildschirmsperre

Organisatorische Maßnahme	Beispiel
Schulungen	Beschäftigte im sicheren Umgang mit Kundendaten unterweisen
Berechtigungsprozess	Rechte bei Eintritt, Wechsel und Austritt anpassen
Löschkonzept	Festlegen, wann welche Daten gelöscht werden
Meldeverfahren	Ansprechpartner und Ablauf für Datenschutzvorfälle festlegen

Datenschutzverletzungen

Eine Datenschutzverletzung kann beispielsweise vorliegen, wenn:

- personenbezogene Daten an einen falschen Empfänger gesendet werden,
- ein unverschlüsseltes Notebook mit Kundendaten verloren geht,
- personenbezogene Daten unberechtigt verändert oder gelöscht werden,
- Angreifer auf eine Kundendatenbank zugreifen.

Richtiges Verhalten als IT-Mitarbeiter

1. Vorfall unverzüglich intern melden.
2. Nach dem vorgesehenen Ablauf den Schaden begrenzen.
3. Wichtige Informationen und Beweise sichern.
4. Zuständige Personen bei der Untersuchung unterstützen.

Meldung an die Aufsichtsbehörde

Meldepflichtige Datenschutzverletzungen müssen unverzüglich und möglichst innerhalb von **72 Stunden nach Bekanntwerden** gemeldet werden.

Eine Meldung ist nicht erforderlich, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Bei voraussichtlich **hohem Risiko** müssen grundsätzlich zusätzlich die betroffenen Personen unverzüglich informiert werden.

Wichtig: Nicht jeder Datenschutzverstoß ist eine meldepflichtige Datenpanne. Als Mitarbeiter sollst du mögliche Vorfälle trotzdem sofort intern melden, damit die zuständige Stelle sie bewerten kann.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter berät und überwacht die Einhaltung des Datenschutzes.

Typische Aufgaben:

- Beschäftigte und Unternehmensleitung beraten,
- Datenschutzmaßnahmen überprüfen,
- Schulungen unterstützen,
- als Ansprechpartner für Datenschutzfragen dienen.

Die Verantwortung für eine rechtmäßige Verarbeitung bleibt beim Unternehmen beziehungsweise der verantwortlichen Stelle.

Eckdatum für Deutschland

Nach dem BDSG besteht eine Benennungspflicht grundsätzlich, wenn in der Regel mindestens **20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind**.

Weitere gesetzliche Fälle können eine Benennung auch unterhalb dieser Zahl erforderlich machen.

Wichtig: Es geht nicht pauschal um 20 Beschäftigte insgesamt.

Übungsfrage: Nennen Sie drei Pflichten eines Unternehmens beim Datenschutz.

Musterantwort: Daten auf einer gültigen Rechtsgrundlage verarbeiten, Betroffene verständlich informieren und die Daten durch geeignete Maßnahmen schützen.

Übungsfrage: Eine Kundenliste wurde versehentlich an einen falschen Empfänger gesendet. Was tun Sie zuerst?

Musterantwort: Den Vorfall sofort nach dem betrieblichen Meldeverfahren intern melden und Maßnahmen zur Schadensbegrenzung einleiten lassen.

Übungsfrage: Welche Frist ist bei einer meldepflichtigen Datenschutzverletzung wichtig?

Musterantwort: Die Meldung an die zuständige Aufsichtsbehörde muss unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden erfolgen.

Übungsfrage: Welche Aufgabe hat ein Datenschutzbeauftragter?

Musterantwort: Er berät zum Datenschutz und überwacht die Einhaltung der Datenschutzvorschriften.

Bedeutung für die Praxis

Für Fachinformatiker ist Datenschutz besonders wichtig beim Einrichten, Betreiben und Warten von IT-Systemen.

Webseiten - Cookies und Tracking

Cookies können beispielsweise eine Anmeldung ermöglichen oder das Verhalten von Besuchern erfassen.

Beispiel	Einordnung
Cookie für eine ausdrücklich gewünschte Warenkorbfunktion	Kann unbedingt erforderlich sein.
Cookie zur seitenübergreifenden Werbefollowung	Ist normalerweise nicht unbedingt erforderlich und benötigt grundsätzlich eine vorherige Einwilligung.

Praktische Maßnahmen

- Nicht erforderliche Tracking-Funktionen erst nach entsprechender Einwilligung aktivieren.
- Ablehnung und Widerruf ermöglichen.
- Verständlich über die Verarbeitung informieren.
- Nur notwendige Daten erheben.

Wichtig: Nicht jeder Cookie benötigt automatisch eine Einwilligung. Für das Speichern und Auslesen auf Endgeräten ist in Deutschland zusätzlich insbesondere das TDDDG relevant.

Übungsfrage: Darf ein Werbetacking-Cookie einfach vor der Zustimmung aktiviert werden?

Musterantwort: Grundsätzlich nein. Für nicht erforderliches Werbetacking ist normalerweise vorher eine wirksame Einwilligung erforderlich.

Kunden- und Mitarbeiterdaten

Typische Daten sind:

- Kontaktdaten,
- Bestellungen,
- Personalnummern,
- Bankverbindungen,

- Gehalts- und Arbeitszeitdaten.

Praktische Maßnahmen

- Zugriffsrechte nach Aufgaben vergeben.
- Keine gemeinsamen Benutzerkonten verwenden.
- Daten nicht ohne Berechtigung weitergeben.
- Bildschirm beim Verlassen des Arbeitsplatzes sperren.
- Ausdrücke mit vertraulichen Daten sicher aufbewahren und entsorgen.
- Nicht mehr erforderliche Berechtigungen entfernen.

Beispiel: Die Personalabteilung benötigt Zugriff auf Gehaltsdaten. Andere Abteilungen erhalten diesen Zugriff nicht allein deshalb, weil sie im selben Unternehmen arbeiten.

Übungsfrage: Warum sollten nicht alle Mitarbeiter Zugriff auf den Personalordner haben?

Musterantwort: Darin befinden sich personenbezogene und teilweise besonders sensible Daten. Zugriff dürfen nur Personen erhalten, die ihn für ihre Aufgaben benötigen.

Cloud-Dienste

Bei Cloud-Diensten werden Daten auf Systemen eines Dienstleisters verarbeitet.

Beispiel: Ein Unternehmen speichert Kundendokumente in einer gehosteten Dateiablage.

Darauf ist zu achten

- Einen geeigneten Anbieter auswählen.
- Zugriffsrechte und Freigaben prüfen.
- Sichere Anmeldung und Verschlüsselung einsetzen.
- Bei Auftragsverarbeitung einen passenden Vertrag abschließen.
- Speicherorte und mögliche Zugriffe aus Drittländern prüfen.
- Löschung, Datenausgabe und Wiederherstellung klären.

Auftragsverarbeitung einfach erklärt

Ein Dienstleister verarbeitet personenbezogene Daten im Auftrag und nach Weisung eines Unternehmens.

Beispiel: Ein Anbieter betreibt das gehostete Kundensystem für ein Unternehmen.

Wichtig: Die Nutzung einer Cloud ist nicht automatisch unzulässig. Entscheidend ist, ob die rechtlichen und technischen Anforderungen erfüllt werden. Ein EU-Speicherort allein beantwortet noch nicht alle Datenschutzfragen.

Übungsfrage: Nennen Sie drei Punkte, die bei der Speicherung von Kundendaten in einer Cloud geprüft werden sollten.

Musterantwort: Zugriffsrechte und Sicherheitsmaßnahmen, der Vertrag zur Auftragsverarbeitung sowie Speicherorte und mögliche Zugriffe aus Drittländern.

IT-Systeme und Datenbanken

Personenbezogene Daten befinden sich häufig in:

- Benutzerverzeichnissen,
- Kundendatenbanken,
- Ticketsystemen,
- Protokolldateien,
- Sicherungskopien.

Praktische Maßnahmen

- Persönliche Konten und passende Berechtigungen einrichten.
- Sicherheitsupdates installieren.
- Übertragungen verschlüsseln.
- Backups gegen unbefugten Zugriff schützen.
- Löschfristen auch bei Protokollen und Sicherungen berücksichtigen.
- Für Tests möglichst künstliche oder ausreichend anonymisierte Daten verwenden.

Beispiel: Für die Prüfung eines neuen Ticketsystems werden erfundene Kundendaten verwendet. Echte Kundendaten werden nicht ohne passende Grundlage in ein ungeschütztes Testsystem kopiert.

Übungsfrage: Warum müssen auch Backups mit Kundendaten geschützt werden?

Musterantwort: Weil die Sicherungskopien ebenfalls personenbezogene Daten enthalten. Auch dort müssen unbefugter Zugriff und unzulässige Nutzung verhindert werden.

Zusammenhängende Übungsaufgabe

Sie richten einen Arbeitsplatz für eine neue Mitarbeiterin ein. Die Mitarbeiterin bearbeitet Kundenanfragen und benötigt Zugang zu einem Ticketsystem.

Nennen Sie vier Maßnahmen, mit denen Sie den Datenschutz unterstützen.

Musterlösung anzeigen

- Ein persönliches Benutzerkonto einrichten.
- Nur die für die Kundenbetreuung erforderlichen Zugriffsrechte vergeben.
- Eine automatische Bildschirmsperre und eine sichere Anmeldung einrichten.
- Die Mitarbeiterin in den sicheren Umgang mit Kundendaten und die internen Meldewege einweisen.

Weitere passende Maßnahmen sind aktuelle Software, verschlüsselte Übertragungen und ein angemessener Schutz lokal gespeicherter Daten.

Wichtige Eckdaten

Thema	Merkwert
Anwendung der DSGVO	Seit 25. Mai 2018
Räumliche Grundlage	Unmittelbare Geltung in allen EU-Mitgliedstaaten
Ergänzung in Deutschland	BDSG
Antwort auf Anträge zu Betroffenenrechten	Grundsätzlich unverzüglich, spätestens innerhalb eines Monats
Meldepflichtige Datenschutzverletzung	Unverzüglich, möglichst innerhalb von 72 Stunden nach Bekanntwerden
Datenschutzbeauftragter nach der allgemeinen BDSG-Schwelle	In der Regel mindestens 20 Personen ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigt; weitere Benennungsgründe beachten

Typische Verwechslungen

Aussage	Richtigstellung
„Für jede Verarbeitung brauche ich eine Einwilligung.“	Es gibt auch andere Rechtsgrundlagen, beispielsweise Vertragserfüllung.
„Eine Datenschutzerklärung erlaubt die Verarbeitung.“	Information allein ersetzt keine Rechtsgrundlage.
„Nach einer Löschanfrage muss sofort alles gelöscht werden.“	Beispielsweise gesetzliche Aufbewahrungspflichten können entgegenstehen.
„Daten ohne Namen sind immer anonym.“	Auch Nummern und andere Angaben können eine Zuordnung ermöglichen.
„Datenschutz und Datensicherheit sind dasselbe.“	Datenschutz regelt den Umgang mit personenbezogenen Daten; Datensicherheit schützt Daten technisch und organisatorisch.
„Der Datenschutzbeauftragte ist allein verantwortlich.“	Die Verantwortung bleibt bei der verantwortlichen Stelle.

Aussage	Richtigstellung
„Jeder Cookie benötigt eine Zustimmung.“	Für unbedingt erforderliche Funktionen können Ausnahmen gelten.

Hinweise für kurze Prüfungsantworten

Achte darauf, was die Aufgabe verlangt:

- **Nennen:** Begriffe oder Maßnahmen aufzählen.
- **Beschreiben:** Kurz erklären, was etwas bedeutet oder wie es funktioniert.
- **Begründen:** Erklären, warum eine Maßnahme in der Situation sinnvoll ist.
- **Unterscheiden:** Den wesentlichen Unterschied deutlich machen.

Beispiel

Aufgabe: „Nennen Sie zwei Maßnahmen zum Schutz von Kundendaten.“

Antwort: „Zugriffsrechte beschränken und Daten verschlüsseln.“

Aufgabe: „Begründen Sie die Beschränkung von Zugriffsrechten.“

Antwort: „Dadurch können nur berechtigte Mitarbeiter auf die Kundendaten zugreifen.“

Die genaue Bewertung richtet sich nach der jeweiligen Aufgabe. Eine kurze Antwort sollte alle verlangten Punkte enthalten.

Kurzmerksatz

Datenschutz schützt Menschen beim Umgang mit ihren personenbezogenen Daten und gibt ihnen Rechte gegenüber den verarbeitenden Stellen.

Zum Einprägen

Nur mit Rechtsgrundlage – nur für einen festgelegten Zweck – nur so viele Daten wie nötig – nur so lange wie erforderlich – angemessen geschützt.
