
Lerneinheit

# [Schutz personenbezogener Daten]

*Projekt: B-SAFE*
*Nummer: 2018-1CZ01-KA204-048148*

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

# Das Thema

**Einführung**

Daten sind wertvoll, und die Möglichkeiten der Datenerfassung und -verarbeitung haben im digitalen Zeitalter rapide zugenommen. Deshalb ist der Datenschutz ein Thema, das uns alle betrifft. Wussten Sie, dass die europäischen Datenschutzbehörden seit der Verabschiedung eines bahnbrechenden EU-Datenschutzgesetzes im Mai 2018 mehr als 95.000 Beschwerden über mögliche Datenschutzverletzungen erhalten hat?

Möchten auch Sie gegebenenfalls Ihre Datenschutzrechte geltend machen können? Dann sind Grundkenntnisse über den Schutz von Personendaten eine wichtige Voraussetzung! Darüber hinaus können Datenverletzungen für Unternehmen existenzbedrohende Folgen haben, weshalb Sie als ArbeitnehmerInnen Grundkenntnisse im Datenschutz haben müssen.

**Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten**

Nach Abschluss dieser Content-Einheit verfügen Sie über ein grundlegendes Verständnis von Datenschutz und Datensicherheit, so dass Sie in der Lage sind, die Datenschutzbestimmungen in Ihrem Berufsleben einzuhalten und als Privatperson mehr Kontrolle über Ihre eigenen Daten zu erlangen.

Co-funded by the
Erasmus+ Programme
of the European Union

# 1.Wissen aufbauen - Zweck des Datenschutzes und europäische Rechtsgrundlagen

In Zeiten zunehmender Digitalisierung und mit dem Aufkommen der Datenwirtschaft ist der Schutz personenbezogener Daten eines der zentralen Themen. Umso entscheidender ist es, dass alle wissen, wofür der Begriff **Datenschutz** eigentlich steht.

| Definition |
| --- |
| Der Datenschutz, auch Informationsschutz genannt, ist ein Aspekt der Datensicherheit, der sich mit dem richtigen Umgang mit personenbezogenen Daten befasst. Er bezieht sich in erster Linie auf den Schutz der persönlichen Daten des Einzelnen vor Missbrauch. |

Datenschutz kann somit als das Recht interpretiert werden, selbst zu entscheiden,

- wer
- zu welcher Zeit und
- in welchem Umfang

Zugang zu Ihren persönlichen Daten hat.

Der Zweck des Datenschutzes besteht also darin, die **Privatsphäre des Einzelnen** zu gewährleisten.

Wussten Sie, dass der Schutz personenbezogener Daten seit Jahren ein **Grundrecht** in Europa ist? In den letzten Jahren ist der Datenschutz in der Praxis jedoch noch wichtiger geworden. Technische Entwicklungen und die globale Vernetzung erleichtern die Erhebung, Verarbeitung, Speicherung, Verbreitung und Analyse von Daten.

| Beispiel |
| --- |
| In den USA gibt es bereits einige sehr erfolgreiche Unternehmen, die sich auf die Erhebung personenbezogener Daten spezialisiert haben. Die Aufzeichnungen umfassen z.B. Name, Geschlecht, politische Zugehörigkeit, Einkommen und vieles mehr. Banken, Versicherungen oder andere Unternehmen kaufen diese Daten, um Hintergrundinformationen zu erhalten, Kreditentscheidungen zu treffen oder Marketingaktivitäten zu optimieren. |

Vielleicht ist Ihnen der Skandal um Cambridge Analytics bekannt, das solche Daten benutzt haben soll, um die Wahlen von US-Präsident Trump maßgeblich zu beeinflussen?

Beispiele wie diese zeigen deutlich, dass Datenschutz wichtig ist, damit die Menschen die **Kontrolle** über ihre persönlichen Daten **behalten**. Daher ist das Hauptziel der **Allgemeinen Datenschutzverordnung (GDPR)** der Schutz **personenbezogener Daten**.

Seit dem 25. Mai 2018 ist das GDPR in Kraft.

Als europäische Regelung ist sie in **jedem europäischen Mitgliedsstaat** unmittelbar - d.h. verbindlich - anwendbar. Nationale Gesetze haben daher nur ergänzenden Charakter. Das GDPR enthält aber auch gewisse Öffnungsklauseln (z.B. können Altersgrenzen durch nationale Gesetze verschoben werden).

Was genau ist das GDPR? Es handelt sich um eine rechtsverbindliche Regelung zum Schutz natürlicher Personen bei der Verarbeitung **personenbezogener Daten**. Der Schutz von Unternehmensdaten spielt nur dann eine Rolle, wenn es sich um personenbezogene Daten handelt (z.B. Daten von MitarbeiterInnen, KundInnen, LieferantInnen).

GDPR zielt darauf ab, die Rechte des Einzelnen zu stärken, das Datenschutzrecht in der EU zu harmonisieren und die Durchsetzbarkeit des Datenschutzes durch einheitliche Durchsetzung und hohe Bußgelder zu verbessern.

Um Einzelpersonen mehr Kontrolle über ihre persönlichen Daten zu geben, gilt das GDPR nicht nur für die gesamte Verarbeitung personenbezogener Daten **durch Organisationen innerhalb der EU, sondern auch für Organisationen außerhalb der EU**, die Waren und Dienstleistungen für BürgerInnen der EU anbieten. Wenn Sie sich also fragen, ob die strengen Datenschutzrichtlinien der EU auch zum Beispiel für in den USA ansässige Suchmaschinenbetreiber gilt, die ihre Dienste europäischen BürgerInnen oder sozialen Netzwerken wie Facebook anbieten, die Antwort ist ja.

Es ist wichtig, dass Sie mit einigen wichtigen Begriffen vertraut sind, die in GDPR eingeführt wurden. Schauen wir uns diese nun genauer an:

| Definition |
| --- |
| Ein für die **Verarbeitung Verantwortlicher** bzw. eine für die **Verarbeitung Verantwortliche** ist die Person (oder das Unternehmen), die über die Zwecke und Arten der Verarbeitung personenbezogener Daten entscheidet, während ein/e DatenverarbeiterIn personenbezogene **Daten im Auftrag** des für die Verarbeitung Verantwortlichen bzw. des für die Verarbeitung Verantwortlicher verarbeitet (mit Ausnahme der eigenen MitarbeiterInnen des für die Verarbeitung Verantwortlichen bzw. des für die Verarbeitung Verantwortlicher). |

Je nachdem, ob ein/e DatenverarbeiterIn oder ein für die Verarbeitung Verantwortlicher bzw. eine für die Verarbeitung Verantwortliche beteiligt ist (z.B. wenn betroffene Personen ihre Rechte wahrnehmen wollen), kann es bei bestimmten Vorschriften Unterschiede geben.

Das GDPR schreibt auch vor, dass es in jedem Mitgliedsstaat **mindestens eine unabhängige Datenschutzaufsichtsbehörde** geben muss, die für die Überwachung der Anwendung des Datenschutzrechts zuständig ist.

| Wichtig |
| --- |
| Im Falle einer grenzüberschreitenden Datenverarbeitung gilt der Mechanismus der einzigen Anlaufstelle. |

| |
|---|
| Das bedeutet, dass sich EU-BürgerInnen immer bei der **Datenschutzbehörde ihres Mitgliedstaates** beschweren können, unabhängig davon, in welchem Mitgliedstaat die Daten missbraucht wurden. |

Glauben Sie, dass Ihre Persönlichkeitsrechte verletzt worden sind? Dann können Sie eine Beschwerde bei Ihrer nationalen Datenverarbeitungsbehörde einreichen, die befugt ist, eine Reihe von **Sanktionen** zu verhängen.

| Wichtig |
|---|
| Es ist wichtig, darauf hinzuweisen, dass das GDPR **die Strafen** für diejenigen, die gegen die Regeln verstoßen, deutlich erhöht hat. Im Extremfall können diese Bußgelder nun bis zu 20 Millionen Euro oder, im Falle von Unternehmen, bis zu 4% des weltweiten Umsatzes des letzten Geschäftsjahres betragen. |

Mit diesen Zahlen können Sie sich vorstellen, wie viel wichtiger die Einhaltung des Datenschutzes für Unternehmen geworden ist.

# 1.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Worum geht es beim Begriff Datenschutz?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Der Datenschutz wird auch als Informationsschutz bezeichnet.
- Beim Datenschutz geht es in erster Linie um den richtigen Umgang mit vertraulichen Unternehmensdaten und deren Schutz vor Missbrauch.
- Datenschutz kann interpretiert werden als das Recht eines jeden Menschen, selbst zu entscheiden, wer, wann und in welchem Umfang Zugang zu personenbezogenen Daten hat.
- Datenschutz hat nichts mit Datensicherheit zu tun.

## Übung SINGLE CHOICE

Situation: Datenschutz ist wichtig für welchen der folgenden Zwecke?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Der Datenschutz ist wichtig, damit die Banken bessere Kreditentscheidungen treffen können.
- Der Datenschutz ist wichtig, damit die Menschen die Kontrolle über ihre persönlichen Daten behalten.
- Der Datenschutz ist wichtig, damit Unternehmen ihre Marketingaktivitäten optimieren können.
- Datenschutz ist wichtig, damit Unternehmen überhaupt keine persönlichen Daten mehr verarbeiten dürfen.

## Übung MULTIPLE CHOICE

Situation: Was ist das GDPR und unter welchen Bedingungen gilt es?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die GDPR ist eine europäische Verordnung, die in jedem europäischen Mitgliedsstaat direkt anwendbar ist.
- Das GDPR ist eine europäische Verordnung, die von Mitgliedsstaaten, die kein eigenes nationales Datenschutzgesetz haben, freiwillig eingehalten werden kann.
- Das GDPR gilt für alle vertraulichen Unternehmensdaten, wie z.B. Betriebsgeheimnisse oder Preis- und Kostenkalkulationen.
- Das GDPR gilt nur für Unternehmen mit Sitz in einem europäischen Mitgliedsstaat und ist daher nicht auf Facebook, Google oder andere Großunternehmen mit Sitz in den USA anwendbar.
- Ziel des GDPR ist es, die Rechte des Einzelnen zu stärken und das Datenschutzrecht in der EU zu harmonisieren.

## Übung MULTIPLE CHOICE

Situation: Was versteht man unter einem Datenverarbeiter bzw. einer Datenverarbeiterin und was unter einem für die Datenverarbeitung Verantwortlichen bzw. einer für die Datenverarbeitung Verantwortlichen im Sinne des GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Ein/e für die Datenverarbeitung Verantwortliche/r entscheidet über den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten.
- Ein/e DatenverarbeiterIn entscheidet über den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten.
- Ein/e DatenverarbeiterIn verarbeitet Daten im Auftrag des für die Verarbeitung Verantwortlichen.
- Die MitarbeiterInnen eines für die Datenverarbeitung Verantwortlichen bzw. einer für die Datenverarbeitung Verantwortlichen werden in der Regel als DatenverarbeiterIn betrachtet.
- Ein/e für die Datenverarbeitung Verantwortliche/r verarbeitet Daten im Auftrag des Datenverarbeiters bzw. der DatenverarbeiterIn.

## Übung SINGLE CHOICE

Situation: Die Österreicherin Josefa H. ist überzeugt, dass ihre Datenschutzrechte durch die deutsche Firma Easyshop verletzt worden sind. Welche der folgenden Aussagen sind richtig?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Josefa H. muss sich an die Datenschutzbehörde in Deutschland wenden, um ihre Datenschutzrechte geltend zu machen, da Easyshop seinen Sitz in Deutschland hat.
- Die Datenschutzbehörde kann bei schweren Datenschutzverletzungen hohe Strafen von bis zu 20 Millionen Euro verhängen.
- Aufgrund der unterschiedlichen Rechtslage im Bereich des Datenschutzes in Österreich und Deutschland sollte Frau Josefa H. zunächst herausfinden, in welchem der beiden Länder ihre Datenschutzbeschwerde erfolgreicher sein könnte.
- Frau Josefa H. sollte sich auf jeden Fall einen Anwalt suchen, denn als Privatperson können Sie sich leider nicht an Datenaufsichtsbehörden wenden.

Co-funded by the
Erasmus+ Programme
of the European Union

# 2.Wissen aufbauen - Materieller Anwendungsbereich des GDPR

Sie wissen bereits, dass das **GDPR** Anwendung findet, sobald **Personendaten von natürlichen Personen** bearbeitet werden. Der Begriff der **Verarbeitung** wird recht weit ausgelegt.


| Definition |
| --- |
| Nach dem GDPR "verarbeiten" Sie personenbezogene Daten, sobald Sie diese durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung sammeln, erfassen, organisieren, ordnen, speichern, anpassen, ändern, auslesen, abfragen, verwenden, offenlegen, vergleichen, verknüpfen, einschränken, löschen oder vernichten. |

In diesem Zusammenhang spielt es keine Rolle, ob diese Verarbeitung **ganz oder teilweise automatisiert** ist. Das GDPR kann sogar auf die **nicht-automatisierte Verarbeitung** von Personendaten (z.B. in Papierform) Anwendung finden. Dies ist dann der Fall, wenn die Daten **in einem strukturierten Dateisystem** gespeichert sind oder **gespeichert werden sollen**.

Fragen Sie sich, was das GDPR unter einem Dateisystem versteht? Gemäß GDPR stellt bereits jede nach bestimmten Kriterien organisierte Sammlung von Personendaten ein **Filesystem** dar.

| Beispiel |
| --- |
| Zum Anwendungsbereich des GDPR gehören z.B. Fragebögen, Catei-Cards oder Akten, die nach den Namen von Personen sortiert sind.<br><br>Dagegen wird ein Haufen ungeordneter Notizblöcke mit personenbezogenen Daten vom GDPR nur dann erfasst, wenn sie irgendwann einmal strukturiert abgelegt werden sollen. |

Der Hintergrund dieser Regelungen soll sicherstellen, dass das Schutzniveau nicht von den verwendeten Datenverarbeitungstechniken abhängt.

Wenn Sie überlegen, ob Ihr privater Notizblock mit den Telefonnummern von Freunden und Familie unter die GDPR fällt - keine Sorge. Das Datenschutzgesetz **gilt nicht** für Bereiche der Datenverarbeitung

im Rahmen ausschließlich **persönlicher oder familiärer Tätigkeiten**, und es tritt auch nicht in bestimmten Sonderfällen wie Tätigkeiten im Bereich der nationalen Sicherheit in Kraft.

Wie Sie bereits wissen, befasst sich das GDPR mit dem Schutz von Personendaten. Doch wofür genau stehen **Personendaten**?

| Definition |
| --- |
| **Personenbezogene Daten** sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person ("betroffene Person") beziehen. |

Wenn Sie sich die folgenden Beispiele anschauen, werden Sie schnell feststellen, dass **personenbezogene Daten** in der Praxis einfach alles umfassen, **was in irgendeiner Weise einen Bezug zu einer natürlichen Person zulässt.**

| Beispiel |
| --- |
| Beispiele für persönliche Daten:<br>• ein Name<br>• Familienstatus<br>• Geburtsdatum und Alter<br>• eine Privatadresse, eine Telefonnummer, eine E-Mail-Adresse<br>• - Konto- oder Kreditkartennummer |

Allerdings macht es datenschutzrechtlich einen großen Unterschied, ob es zum Beispiel um den Schutz Ihrer E-Mail-Adresse oder Ihrer Krankengeschichte geht. Sogenannte **sensible Daten** erhalten einen erhöhten Schutz.

| Definition |
| --- |
| **Sensible Daten** sind eine **besondere Kategorie** von persönlichen Daten:<br>• Rasse und ethnische Herkunft,<br>• politische Meinung,<br>• religiöse oder philosophische Überzeugungen oder<br>• Gewerkschaftsmitgliedschaft.<br>Dazu gehört auch die Verarbeitung von genetischen oder biometrischen Daten oder Daten über die Gesundheit oder das Sexualleben einer natürlichen Person. |

| Beispiel |
| --- |
| Beispiele für sensible Daten sind medizinische Aufzeichnungen, Fingerabdrücke und Iris-Scans oder religiöse Zeugnisse. |

Diese Daten sind besonders schützenswert. Daher sind die Regeln für die Verarbeitung sensibler Daten äußerst streng.

# 2.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle ist das GDPR anwendbar?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Eine Marketingfirma sammelt Namen und E-Mail-Adressen per Telefonanruf und speichert sie elektronisch.**
- **Ein kleiner Handwerksbetrieb führt eine Kundenliste (Namen und Telefonnummern) in Papierform.**
- Die Beamtin Lisa S. ist Mitglied einer nationalen Sicherheitsbehörde. Im Rahmen ihrer Tätigkeit wertet sie Telefonprotokolle aus.
- **Peter P. ist kürzlich zum Geschäftsführer eines langjährigen Familienunternehmens befördert worden. Er will sich auf neue Geschäftsfelder konzentrieren und löscht deshalb zahlreiche Einträge aus der bestehenden Kundendatenbank.**
- Die Studentin Sarah K. notiert sich die Kontaktdaten mehrerer Kommilitonen.
- **Die Mitarbeiterin Maria S. wertet die Ergebnisse einer schriftlichen Kundenbefragung aus. Die Umfrage wurde mittels Fragebögen in Papierform durchgeführt. Die Kunden wurden gebeten, ihre Postleitzahl anzugeben, die Angabe ihres Namens war jedoch freiwillig.**

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Daten sind personenbezogene Daten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Name einer Person**

- Geburtsdatum
- Adresse einer Person
- Standort des Unternehmens
- Einkommen
- Verkaufszahlen
- Mitarbeiterfoto auf der Firmen-Homepage
- E-Mail-Adressen einer Person
- E-Mail-Adresse eines Unternehmens

### Übung MULTIPLE CHOICE

Situation: Welche der folgenden Daten sind sensible Daten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Fingerabdruck
- Anamnese
- Alter
- Angaben zum Konto
- sexuelle Orientierung
- Gewerkschaftsmitgliedschaft

# 3.Wissen aufbauen - Prinzipien und Bedingungen für die Datenverarbeitung

Das GDPR definiert **sieben Schlüsselprinzipien**, die bei der Datenverarbeitung strikt eingehalten werden müssen:

1. Daten müssen **rechtmäßig, fair und transparent** verarbeitet werden.
2. Daten dürfen nur für **festgelegte, eindeutige und rechtmäßige Zwecke** verarbeitet werden.
3. Die Verarbeitung von Daten muss auf das **unbedingt notwendige Maß beschränkt** werden.
4. Die Daten müssen **sachlich** richtig und auf dem neuesten Stand sein.
5. Personenbezogene Daten müssen in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen **nur so lange ermöglicht, wie es für die Zwecke**, für die sie verarbeitet werden, erforderlich ist.
6. Personenbezogene Daten müssen durch geeignete technische (z.B. Backups) und organisatorische Maßnahmen (z.B. Zugriffsberechtigungen) vor **unbefugter Verarbeitung** und vor zufälligem **Verlust oder Beschädigung geschützt** werden.
7. Der für die **Verarbeitung Verantwortliche** muss die **Einhaltung der Datenschutzgrundsätze nachweisen können**.

| Wichtig |
| --- |
| Verstöße gegen diese Grundsätze werden wahrscheinlich zu **Höchststrafen führen**. |

Wussten Sie, dass die **Verarbeitung personenbezogener Daten generell** verboten ist, es sei denn, bestimmte Bedingungen sind erfüllt? Für nicht-sensible Personendaten stehen im GDPR insgesamt **sechs gesetzliche Grundlagen für die Verarbeitung zur Verfügung**:

1. **Die Verarbeitung ist zur Erfüllung eines Vertrages notwendig** - z.B. die Verarbeitung von Kundenadressdaten bei Online-Käufen

2. **Die Verarbeitung ist erforderlich, um einer gesetzlichen Verpflichtung** - z.B. der Pflicht des Arbeitgebers bzw. der Arbeitgeberin zur Arbeitszeiterfassung - nachzukommen
3. **Die Verarbeitung ist notwendig, um das Leben eines Menschen zu schützen** - z.B. im Falle von Epidemien oder Naturkatastrophen
4. **Personenbezogene Daten werden zur Erfüllung besonderer Aufgaben im Interesse der Öffentlichkeit** oder in Ausübung öffentlicher Gewalt verarbeitet, die gesetzlich vorgesehen sind - z.B. im Rahmen polizeilicher Anfragen
5. Die Verarbeitung ist zur Wahrung Ihrer berechtigten Interessen oder der berechtigten Interessen eines Dritten erforderlich, es sei denn, es besteht ein triftiger Grund, die personenbezogenen Daten des Einzelnen zu schützen, der diese berechtigten Interessen überlagert - z.B. Videoüberwachung des Firmengeländes zum Schutz vor Einbruch
6. Einwilligung der betroffenen Person - z.B. durch Unterschrift oder Ankreuzen eines Kästchens auf einer Website.

| Wichtig |
| --- |
| Einverständniserklärungen können von den Betroffenen **jederzeit widerrufen** werden! |

Wenn die Einwilligung als rechtmäßige Grundlage verwendet werden soll, müssen bestimmte Voraussetzungen erfüllt sein, wobei auch das **Alter der betroffenen Person** zu berücksichtigen ist.

| Wichtig |
| --- |
| Bei Personen, die das **16. Lebensjahr** noch nicht vollendet haben, ist die Zustimmung der Eltern oder des gesetzlichen Vormunds erforderlich. Die EU-Mitgliedsstaaten können eine niedrigere Altersgrenze für die Einholung der elterlichen Zustimmung festlegen, die jedoch nicht unter 13 Jahren liegen darf. |

Für die Verarbeitung **sensibler Daten** gelten besondere Anforderungen. Die Datenverarbeitung ist nur in **bestimmten Ausnahmefällen** zulässig, z.B. bei einem Unfall aufgrund lebenswichtiger Interessen oder wenn die Personendaten offensichtlich von der betroffenen Person veröffentlicht worden sind.

# 3.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Als MitarbeiterIn eines Beratungsunternehmens verarbeiten Sie verschiedene Kundendaten. Was sollten Sie beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Verarbeitung von Personendaten muss auf das unbedingt Notwendige beschränkt werden
- bestehende persönliche Daten dürfen nicht aktualisiert werden
- persönliche Daten dürfen nicht unbegrenzt gespeichert werden
- die Daten müssen vor unbefugter Verarbeitung geschützt werden
- Höchststrafen werden wahrscheinlich im Falle eines Verstoßes gegen grundlegende Datenschutzprinzipien verhängt

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle fällt die Verarbeitung personenbezogener, nicht-sensibler Daten unter eine der sechs Rechtsgrundlagen und ist daher zulässig?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffend sein.

- Ein Kunde bzw. eine Kundin kauft eine neue Küche und möchte sie zu sich nach Hause geliefert bekommen. Der Verkäufer bzw. die Verkäuferin notiert die Adresse der Kundschaft und speichert sie in der Kundendatenbank.
- In einem Unternehmen werden die Arbeitszeiten aller MitarbeiterInnen erfasst und verarbeitet.
- Ein Kunde bzw. eine Kundin stimmt der Verarbeitung seiner/ ihrer persönlichen Daten zu und unterzeichnet eine Einverständniserklärung.
- Ein Sportverein veröffentlicht die Geburtsdaten der Neugeborenen seiner Mitglieder und deren Hochzeitsdaten in einer Vereinszeitung.

## Übung MULTIPLE CHOICE

Situation: Stellen Sie sich vor, Sie möchten personenbezogene Daten verarbeiten. Mangels anderer Rechtsgrundlagen benötigen Sie die Einverständniserklärung der betroffenen Personen. Was müssen Sie beachten?
Die Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Einwilligung kann von der betroffenen Person jederzeit zurückgezogen werden.
- Bei Personen, die das 16. Lebensjahr noch nicht vollendet haben, ist für eine gültige Einwilligung die Zustimmung eines Elternteils oder Erziehungsberechtigten erforderlich.
- Die EU-Mitgliedstaaten können eine höhere Altersgrenze für die Einholung der elterlichen Zustimmung festlegen.
- Die EU-Mitgliedsstaaten können eine niedrigere Altersgrenze für die Einholung der elterlichen Zustimmung festlegen.

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle ist die Verarbeitung sensibler Daten erlaubt?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Eine bewusstlose Person wird nach einem Unfall ins Krankenhaus gebracht. Daten wie Blutgruppe, Alter oder Allergien werden verarbeitet.
- Eine homosexuelle Person spricht in einem Fernsehinterview offen über ihre sexuelle Orientierung.
- In keinem der Fälle, da die Verarbeitung sensibler Daten ausnahmslos streng verboten ist.
- Die Verarbeitung sensibler Daten ist nur in einem Fall erlaubt, nämlich dann, wenn die betroffene Person ihre Einwilligung gibt.

Co-funded by the
Erasmus+ Programme
of the European Union

# 4.Wissen aufbauen - Pflicht zur Benachrichtigung bei Datenverletzungen

Angenommen, Sie beginnen Ihren Arbeitstag wie gewohnt, werden aber plötzlich mit folgenden Ereignissen konfrontiert:

- es hat einen Hackerangriff auf Ihren Firmenserver gegeben, wodurch Unbefugte Zugang zu persönlichen Daten erhalten haben, oder
- es gab einen Einbruch in einen Firmenwagen - Notebooks mit persönlichen Daten wurden gestohlen.

Diese Vorkommnisse stellen eine Bedrohung für den Schutz personenbezogener Daten dar.

| Definition |
| --- |
| Vorfälle, die zu versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Änderung oder unberechtigtem Zugriff auf persönliche Daten führen könnten, werden als **Datenverletzungen bezeichnet.** |


Es ist die Pflicht jedes Datenverarbeiters, den für die Datenverarbeitung Verantwortlichen bzw. die für die Datenverarbeitung Verantwortliche unverzüglich über jede Datenverletzung zu informieren.

| Wichtig |
| --- |
| Bei einer Datenverletzung muss, der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche einer **Melde- und Benachrichtigungspflicht** nachkommen. Dies bedeutet:<br>• Die **Datenschutzbehörde** muss innerhalb von **72 Stunden**, nachdem sie von der Verletzung Kenntnis erlangt hat, informiert werden, wenn dadurch die Rechte und Freiheiten der betroffenen Personen gefährdet werden könnten. |

- - Die **zusätzliche Benachrichtigung der betroffenen Personen** ist immer dann erforderlich, wenn mit einem **hohen Risiko** für die Rechte und Freiheiten der betroffenen Personen zu rechnen ist - z.B. wenn sensible Daten von der Datenverletzung betroffen sind.

# 4.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Was gilt als Datenverletzung im Sinne des GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Unbefugte Personen haben durch einen Hackerangriff Zugriff auf persönliche Daten erhalten.
- Ein Mitarbeiter bzw. eine Mitarbeiterin hat versehentlich zahlreiche Kundendaten gelöscht.
- Ein Laptop mit wichtigen Aussagen über die neue Marketingstrategie des Unternehmens wurde gestohlen.
- Ein Mitarbeiter bzw. eine Mitarbeiterin einer Personalagentur verlor einen USB-Stick, auf dem unter anderem zahlreiche Lebensläufe und Notizen zur persönlichen Situation von KundInnen gespeichert waren.

## Übung MULTIPLE CHOICE

Situation: Bei einer Krankenkasse kam es zu einem Cyber-Angriff. Hacker haben sich Zugang zu zahlreichen Gesundheitsdaten der Versicherten verschafft. Wie ist das Vorgehen nach dem GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehrere oder alle Optionen können wahr sein.

- Es besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, weshalb der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche die betroffene Person auch über diesen Vorfall informieren muss.
- Der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche muss die Datenschutzbehörde innerhalb von 72 Stunden informieren.
- Der/ die DatenverarbeiterIn muss den für die Datenverarbeitung Verantwortlichen bzw. die für die Datenverarbeitung Verantwortliche innerhalb von 72 Stunden benachrichtigen.
- Der/ die DatenverarbeiterIn muss die Datenschutzbehörde innerhalb von 72 Stunden benachrichtigen.
- Da es sich nicht um sensible Daten handelt, reicht es aus, die Datenschutzbehörde zu benachrichtigen. Der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche kann auf die Benachrichtigung der betroffenen Person verzichten.

Co-funded by the
Erasmus+ Programme
of the European Union

# 5.Wissen aufbauen - Rechte der betroffenen Personen

Das GDPR erweitert die Rechte der betroffenen Personen. Sie sollten diese Rechte kennen, damit Sie Ihre Rechte wahrnehmen und bei Datenschutzanfragen an Ihr Unternehmen gesetzeskonform reagieren können. Wie Sie aus der Grafik ersehen können, sieht das GDPR folgende Rechte für natürliche Personen vor:


Aber was bedeuten diese Rechte eigentlich in der Praxis? Schauen wir genauer hin:
Beginnen wir mit dem **Recht, informiert zu werden**. Wenn Ihre **persönlichen Daten verarbeitet werden**, ist der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche verpflichtet, Ihnen zum Zeitpunkt der Erfassung Ihrer Daten **bestimmte Informationen** zu geben, darunter insbesondere:

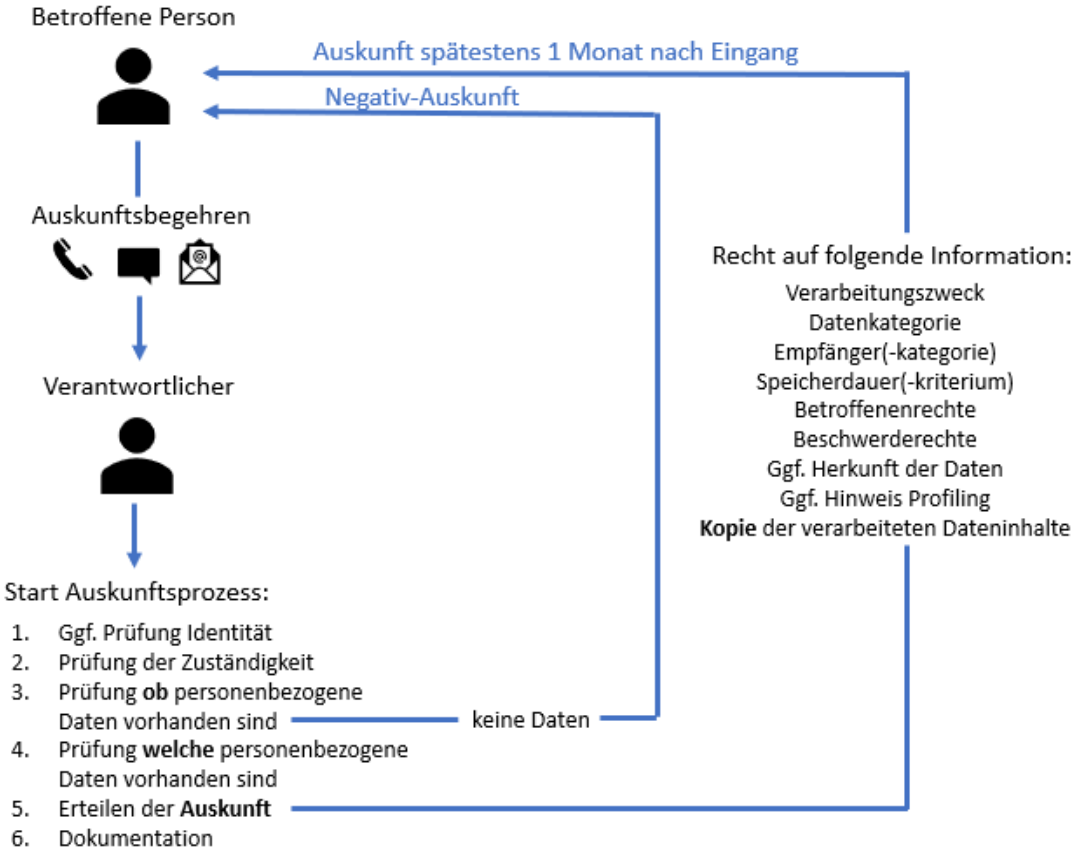
- **wer** Ihre Daten verarbeitet (Name und Kontaktangaben)
- **welche** Daten sie verarbeiten,
- **warum** sie es bearbeiten und
- für **wie lange** die Daten aufbewahrt werden

Darüber hinaus verlangt das GDPR, dass **die Informationen** Ihnen zur Verfügung gestellt werden

- in einer präzisen, transparenten und leicht zugänglichen Form
- in klarer und einfacher Sprache und
- kostenlos

Um dem Recht auf Information gerecht zu werden, müssen die für die Datenverarbeitung Verantwortlichen den Personen **aktiv** bestimmte Informationen zur Verfügung stellen. Im Gegensatz dazu **berechtigt das Auskunftsrecht** jede betroffene Person, eine Kopie ihrer persönlichen Daten und andere ergänzende Informationen über die Datenverarbeitung zu erhalten.

Die folgende Grafik zeigt die richtige Antwort, wenn eine betroffene Person ihr Auskunftsrecht ausüben möchte:




Wie Sie aus der Grafik ersehen können, kann das Auskunftsersuchen persönlich, schriftlich oder telefonisch gestellt werden. Es ist wichtig, die **Identität** der Person, die das Ersuchen stellt, zweifelsfrei zu klären.

Der nächste Schritt ist die **Prüfung der Verantwortlichkeit**.

| Wichtig |
| --- |
| Betroffene Rechte können nur bei der **verantwortlichen Stelle** geltend gemacht werden! Da der/ die DatenverarbeiterIn jedoch eine **Unterstützungspflicht** hat, sollte die **Datenschutzanfrage** direkt an die für die Datenverarbeitung Verantwortlichen weitergeleitet werden.<br>Ohne ausdrückliche Weisung sind Sie als MitarbeiterIn **nicht berechtigt, Auskunft über Personendaten zu erteilen!** |

Wie Sie vielleicht schon aus der Grafik ersehen konnten, müssen die für die Verarbeitung Verantwortlichen dem Antrag auf Ausübung des Auskunftsrechts nachkommen, wenn keine personenbezogenen Daten verarbeitet werden (**Negativinformation**). Werden personenbezogene Daten tatsächlich verarbeitet, haben die Personen jedoch das **Recht, auf diese Daten zuzugreifen**, eine Kopie der verarbeiteten personenbezogenen Daten zu erhalten und alle relevanten Zusatzinformationen zu erhalten.

| Wichtig |
| --- |
| Im Falle eines Datenschutzbegehrens beträgt die Frist für die Auskunftserteilung grundsätzlich **nur einen Monat** nach Eingang des Begehrens. |

| Hinweis |
| --- |
| Die bisher erlernten Regelungen in Bezug auf<br>- Form der Datenschutzanfrage (schriftlich, elektronisch, persönlich, telefonisch) |

- Verpflichtung, im Zweifelsfall die Identität der betroffenen Person zu überprüfen
- Verantwortung des Datenschutzantrags (nur für die Datenverarbeitung Verantwortlichen)
- Frist für die Antwort zum Datenschutz (1 Monat)

gelten gleichermaßen für ALLE Rechte der betroffenen Personen!

**Das Recht auf Berichtigung** gibt Einzelpersonen das Recht, die Berichtigung unrichtiger, ungenauer oder unvollständiger personenbezogener Daten zu verlangen.

Der Einzelne kann **die Löschung von Personendaten** verlangen, wenn beispielsweise die vom Unternehmen verarbeiteten Daten nicht mehr benötigt werden oder wenn die Daten unrechtmäßig verwendet worden sind. Dieses Recht gilt auch **online** und wird oft als das **"Recht, vergessen zu werden"** bezeichnet. Dieses Recht verpflichtet die für die Datenverarbeitung Verantwortlichen, alle angemessenen Schritte zu unternehmen, um öffentlich bekannt gegebene personenbezogene Daten zu entfernen.

**Das Recht, die Verarbeitung einzuschränken**, ist ein Recht, das nur **unter bestimmten Bedingungen** ausgeübt werden kann. Beispiele hierfür sind der Einspruch einer betroffenen Person gegen die Datenverarbeitung, wobei die Entscheidung über den Einspruch noch aussteht, oder ein Streit über die Richtigkeit der Daten.

**Das Recht auf Datenportabilität** soll sicherstellen, dass Einzelpersonen die Übermittlung der von ihnen zur Verfügung gestellten personenbezogenen Daten in einem strukturierten, gemeinsamen und maschinenlesbaren Format an einen für die Datenverarbeitung Verantwortlichen beantragen können. Das Recht gilt nur, wenn die Daten auf der Grundlage einer Einwilligung oder eines Vertrages verarbeitet werden. Sie können auch verlangen, dass personenbezogene Daten direkt an einen anderen für die Datenverarbeitung Verantwortlichen übermittelt werden, wenn dies technisch machbar ist.

| Beispiel |
| --- |
| Angenommen, Sie möchten Ihren E-Mail-Provider wechseln. **Das Recht auf Datenübertragbarkeit** ermöglicht es Ihnen, Ihren derzeitigen E-Mail-Provider zu bitten, Ihre Kontaktliste an einen neuen E-Mail-Provider zu senden. |

Grundsätzlich haben die betroffenen Personen **das Recht, gegen die Verarbeitung** personenbezogener Daten Widerspruch einzulegen. Ob dieses Recht gilt, hängt vom Zweck und der rechtmäßigen Grundlage der Verarbeitung ab. Beispielsweise haben Sie immer das Recht, der Verarbeitung zum Zweck der Direktwerbung zu widersprechen. Werden Daten jedoch beispielsweise für wissenschaftliche oder historische Forschung oder für statistische Zwecke verarbeitet, ist das Widerspruchsrecht eingeschränkter.

Das GDPR gibt Einzelpersonen **das Recht, sich nicht einer Entscheidung zu unterwerfen**, **die ausschließlich auf einer automatisierten Verarbeitung**, einschließlich der Erstellung von Profilen, beruht.

| Wichtig |
| --- |
| Nur **natürliche Personen** haben Anspruch auf Ausübung der Datenschutzrechte! Die Ausübung der Rechte der betroffenen Personen muss **unentgeltlich** sein. Die Nichteinhaltung dieser Rechte kann zu hohen Geldstrafen führen. |

Co-funded by the
Erasmus+ Programme
of the European Union

# 5.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Mit dem GDPR werden die Rechte des Einzelnen gestärkt. Auf welche Rechte kann sich der Einzelne nun berufen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Recht auf Einspruch
- Recht auf Information
- Recht auf Veröffentlichung
- Recht auf Datenportabilität
- Recht auf Berichtigung
- Recht auf Zugang
- Recht auf gerechte Bezahlung für Daten

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen über das Recht auf Information und das Auskunftsrecht sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- Das Auskunftsrecht gibt den betroffenen Personen das Recht, eine Kopie ihrer verarbeiteten Personendaten zu erhalten.
- Das Recht auf Information ist genau dasselbe wie das Auskunftsrecht.
- Das Auskunftsrecht bedeutet, dass die um Auskunft ersuchende Person auch das Recht hat, darüber informiert zu werden, dass keine sie betreffenden Personendaten bearbeitet werden (Negativinformation).
- Das Recht auf Information bedeutet, dass der/die für die Datenverarbeitung Verantwortliche die betroffenen Personen aktiv über bestimmte Punkte der Datenverarbeitung informieren muss.

## Übung SINGLE CHOICE

Situation: Ein/e KundeIn kontaktiert Sie telefonisch. Er/ Sie möchte wissen, welche Daten von ihm/ ihr in Ihrem Unternehmen verarbeitet werden. Wie reagieren Sie darauf?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Ich beantworte seine Anfrage sofort.
- Ich beantworte seine Anfrage, wenn ich die Kundschaft kenne und keine sensiblen Daten von ihm verarbeitet werden.
- Ich werde die Anfrage beantworten, wenn ich die Kundschaft kenne.
- Ich teile der Person mit, dass ich persönlich als MitarbeiterIn ohne ausdrückliche Weisung keine Auskünfte erteilen darf und bitte, seine/ ihre Anfrage schriftlich an die Verantwortlichen für die Datenverarbeitung zu richten.

Co-funded by the
Erasmus+ Programme
of the European Union

## Übung SINGLE CHOICE

Situation: Wer ist laut DSGVO für die Beantwortung von Datenschutzanfragen von Betroffenen zuständig?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- BearbeiterIn der Daten
- Verantwortliche für die Datenverarbeitung
- Angestellte, wenn sie die betreffende Person zweifelsfrei identifizieren können
- Nur die Datenschutzbehörde

## Übung MULTIPLE CHOICE

Situation: Herr P. erhält seit einigen Wochen Postsendungen von einem Unternehmen, das ihm nicht bekannt ist. Er beschließt daher, dieses Unternehmen telefonisch um Auskunft darüber zu bitten, welche persönlichen Daten das Unternehmen über ihn hat und woher das Unternehmen diese Daten erhalten hat.
Welche der folgenden Aussagen ist richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- Das Unternehmen kann Herrn P. um einen Identitätsnachweis bitten, bevor es auf sein Auskunftsersuchen antwortet.
- Wenn Herr P. innerhalb eines Monats keine Antwort oder Informationen vom Unternehmen erhält, kann er bei der Datenschutzbehörde eine Beschwerde einreichen.
- Herr P. kann sein Auskunftsrecht nur persönlich vor Ort, gegen Vorlage eines Personalausweises, geltend machen.
- Das Unternehmen ist berechtigt, für die Übermittlung von Informationen in Papierform eine Gebühr zu verlangen. Lediglich die Übermittlung in elektronischer Form muss für den Auskunftsuchenden kostenfrei sein.

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen zum Recht auf Datenportabilität sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- Einzelpersonen können die Übermittlung der personenbezogenen Daten, die sie einer für die Datenverarbeitung verantwortlichen Person zur Verfügung gestellt haben, beantragen.
- Das Recht gilt nur, wenn die Daten auf der Grundlage einer Einwilligung oder eines Vertrages verarbeitet werden.
- Auch Unternehmen können das Recht auf Datenportabilität geltend machen.
- Das Recht auf Datenübertragbarkeit ermöglicht es Ihnen, Ihren derzeitigen E-Mail-Provider zu bitten, Ihre Kontaktliste an einen neuen E-Mail-Provider zu senden. Die Kosten der Datenübermittlung gehen zu Lasten des neuen E-Mail-Providers.
- Die Nichteinhaltung dieses Rechts kann zu hohen Geldstrafen führen.

Co-funded by the
Erasmus+ Programme
of the European Union

## Übung MULTIPLE CHOICE

Situation: Klaus heiratete im vergangenen Jahr und stimmte zu, dass der Fotograf Hochzeitsfotos zu Werbezwecken auf seiner Firmenwebsite veröffentlichen darf. Heute ist Klaus geschieden und er ärgert sich darüber, dass durch die Eingabe seines Namens bei Google seine Hochzeitsfotos für jedermann sichtbar sind. Welche der folgenden Aussagen sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehrere oder alle Optionen können wahr sein.

- Er hat das Recht, seine Zustimmung zur Datenverarbeitung durch den Hochzeitsfotografen zu widerrufen.
- Er hat auch das Recht zu verlangen, dass seine im Internet veröffentlichten Fotos gelöscht werden.
- Klaus Ex-Frau Lisa ist ausgezogen. Sie hat das Recht, eine Korrektur ihrer Kundendaten zu verlangen (neue Adresse).
- Das Recht, die Bearbeitung einzuschränken, erlaubt es den Hochzeitsfotografen, die Fotos weiterhin für Werbezwecke zu verwenden.

# 6.Wissen aufbauen - Maßnahmen zur Datensicherheit

Um den Schutz der persönlichen Daten zu gewährleisten, spielt die Frage der **Datensicherheit** sicherlich eine zentrale Rolle. Wichtige Stichworte in diesem Zusammenhang sind **Privacy by Design** und **Privacy by Default**.

| Definition |
|---|

Co-funded by the
Erasmus+ Programme
of the European Union

Der Begriff **Privacy by Design** bezieht sich auf den Datenschutz durch **Technologiegestaltung**. Das bedeutet, dass bei der Entwicklung neuer Technologien auf angemessene und datenschutzkonforme Lösungen geachtet werden muss. Beispielsweise dürfen wichtige Datenschutzprinzipien, wie die Datenminimierung, bei der Entwicklung neuer Softwareprogramme und Geräte nicht ignoriert werden.

**Privacy by default** steht für Datenschutz durch entsprechende **Voreinstellungen**. Die verantwortliche Person muss durch entsprechende Voreinstellungen sicherstellen, dass nur diejenigen Personendaten verarbeitet werden, die absolut notwendig sind.

Sind Sie sich immer noch nicht sicher, was Datenschutz by design and default eigentlich bedeutet? Schauen wir uns ein paar Beispiele an:

| Beispiel |
| --- |
| **Datenschutz durch Design**: Integration von Löschkonzepten in Software zur Datenverarbeitung oder die Verwendung von Pseudonymisierung (Ersetzen von persönlich identifizierbarem Material durch künstliche Identifikatoren) und Verschlüsselung (Verschlüsselung von Nachrichten, so dass nur die Berechtigten sie lesen können).<br><br>**Datenschutz als Standard**: Beispielsweise muss ein/e AnbieterIn eines sozialen Netzwerks durch die Voreinstellung seiner App von vornherein sicherstellen, dass persönliche Daten der NutzerInnen nicht veröffentlicht werden. Personen, die die App nutzen, sollten nicht erst die Einstellungen von "öffentlich" auf "privat" ändern müssen. |

Doch was kann konkret getan werden, um die Datensicherheit zu verbessern? Im Folgenden lernen Sie einige geeignete Maßnahmen auf einen Blick kennen:

- **Definition der Datenschutzziele**
- **TOMs - technische und organisatorische Maßnahmen**

Schauen wir uns nun die einzelnen Maßnahmen etwas näher an:

Als wesentliche Datenschutzziele gelten

- **Integrität (Integrity)**: Die Daten sind originalgetreu und wurden nicht von Unbefugten beschädigt oder verändert.
- **Verfügbarkeit (Availability)**: Die Daten stehen autorisierten Personen zur Verfügung, wann und wo sie sie benötigen. Das Datenverarbeitungssystem ist bis zu einem gewissen Grad tolerant gegenüber Fehlfunktionen und Fehlern.
- **Vertraulichkeit (Confidentiality)**: Die Daten sind nur autorisierten Personen zugänglich.

Co-funded by the
Erasmus+ Programme
of the European Union


Das GDPR verlangt, dass die für die Verarbeitung Verantwortlichen und die **AuftragsverarbeiterInnen geeignete technische und organisatorische Maßnahmen** (TOMS) bei der Datenverarbeitung ergreifen müssen, um ein dem Risiko angepasstes Schutzniveau zu gewährleisten.

Wie Sie bereits wissen, verpflichtet das GDPR zum Schutz der **Privatsphäre per Design und Standard**.

Die genauen Maßnahmen, die zum Schutz personenbezogener Daten zu ergreifen sind, liegen jedoch letztlich in der Verantwortung der für die Verarbeitung Verantwortlichen und der AuftragsverarbeiterInnen. Beispiele für TOMs sind Pseudonymisierung und Verschlüsselung von Daten, Information und Schulung des Personals oder automatische Backups.

Das folgende Beispiel zeigt, wie Datenschutzmaßnahmen in der Praxis umgesetzt werden können.

**Beispiel**

Angenommen, Sie sind bei einem Unternehmen beschäftigt, das eine **Kundendatenbank** verwendet. Diese Kundendatenbank befindet sich auf einem Server. Um ein angemessenes Schutzniveau für die persönlichen Daten der KundeInnen zu gewährleisten, wären z.B. die folgenden Datenschutzmaßnahmen denkbar:

- Der Zugriff auf alle KundInnendaten ist nur mit **Passwort und Benutzername** möglich.
- Der Raum, in dem sich der Server befindet, wird mit einem **Schlüssel verschlossen**.
- Jede **Benutzung** wird protokolliert, sowohl An- und Abmeldung als auch Änderungen an Datensätzen. Jedem Login ist eine Person zugeordnet.
- **Lese- und Schreibrechte** werden nur nach Bedarf vergeben.
- KundInnen werden nach Möglichkeit nicht unter einem realen Namen, sondern unter einer **Benutzerkennung** erfasst.
- Es werden regelmäßig **Backups** erstellt, die ebenfalls in bestimmten Zeitabständen auf ihre Integrität geprüft werden.
- Alle **TOMs** werden vierteljährlich **überprüft**.
- - Die MitarbeiterInnen erhalten klare Anweisungen zum Umgang mit persönlichen Daten, eine **Grundschulung zum Datenschutz und regelmäßige spezifische Datenschutzhinweise per E-Mail.**

Co-funded by the
Erasmus+ Programme
of the European Union

# 6.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Was ist mit den Begriffen "privacy for design" und "privacy by default" gemeint?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Privacy by design steht für Datenschutz durch entsprechende Voreinstellungen.
- Privacy by default steht für Privatsphäre durch geeignete Voreinstellungen.
- Privacy by design steht für Datenschutz durch Technologieentwicklung.
- Eine App ist so voreingestellt, dass persönliche Daten von anderen BenutzerInnen nicht eingesehen werden können. Dies ist ein Beispiel für Privacy by default.
- In einem Softwareprogramm werden alle nicht unbedingt notwendigen Daten anonymisiert gespeichert. Dies ist ein Beispiel für den standardmäßigen Datenschutz.

## Übung MULTIPLE CHOICE

Situation: Was sind die wichtigen Schutzziele im Datenschutz?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Integrität
- Verfügbarkeit von Daten
- Offener Datenzugang
- Vertraulichkeit
- Hohe Lagerdauer
- Daten-Transparenz

## Übung MULTIPLE CHOICE

Situation: Was ist mit dem Begriff TOM gemeint und wer ist nach dem GDPR für deren Umsetzung verantwortlich?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Abkürzung TOMs steht für technische und organisatorische Maßnahmen zum Datenschutz.
- Das Kürzel TOMs steht für technisch zwingende Maßnahmen zum Datenschutz.
- Die für die Datenverarbeitung Verantwortlichen und die DatenverarbeiterInnen sind für die Umsetzung geeigneter TOMs verantwortlich.
- Die für die Datenverarbeitung Verantwortlichen sind für die Implementierung geeigneter TOMs verantwortlich.
- Die Datenschutzbehörde ist für die genauen Maßnahmen verantwortlich, die zum Schutz der persönlichen Daten getroffen werden müssen.
- Die Schulung von MitarbeiterInnen ist ein Beispiel für die Umsetzung von Datenschutzbestimmungen.
- Automatische Back-ups oder Pseudonymisierung sind Beispiele für TOMs.

Co-funded by the
Erasmus+ Programme
of the European Union

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Maßnahmen können in der Praxis für den Datenschutz eingesetzt werden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehrere oder alle Optionen können wahr sein.

- Regelmäßige Sicherungen.
- Grundschulung zum Datenschutz für alle MitarbeiterInnen.
- Um Zugang zu Kundendaten zu erhalten, benötigen Sie ein Passwort und einen Benutzernamen.
- Wenn möglich, werden KundInnen unter ihrem echten Namen und nicht unter einer BenutzerInnen-ID erfasst.
- So viele Daten wie möglich werden so lange wie technisch möglich gespeichert.

# 7. Datenschutzrechtliche Maßnahmen - was können SIE tun?

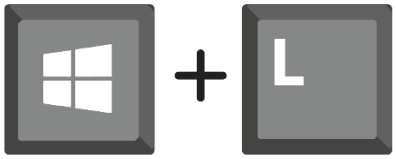
Neben der technischen Komponente ist auch **die personelle Komponente** besonders wichtig. Informieren Sie sich jetzt, wie **Sie** zu einem besseren Datenschutz in Ihrem Unternehmen beitragen können:

Eine wichtige Datenschutzmaßnahme ist die sogenannte **Clear Desk/Clear Screen Policy**.

| Definition |
| --- |
| **Die Clear Desk Policy** bezieht sich auf die Anweisung, dass MitarbeiterInnen alle vertraulichen Dokumente bei Abwesenheit verschließen und sie am Arbeitsplatz nicht offen liegen lassen. Damit soll verhindert werden, dass unbefugte Personen (wie BesucherInnen, KundInnen, Reinigungspersonal) Zugang zu ihnen erhalten. |

Darüber hinaus sollten alle MitarbeiterInnen ermutigt werden, eine **klare Bildschirmrichtlinie** zu verabschieden. Dies bedeutet, dass alle BenutzerInnen verpflichtet sind, sich beim Verlassen des Arbeitsplatzes vom PC abzumelden oder den PC zu sperren, wenn es nur zu kurzen Unterbrechungen kommt.

| Tipp |
| --- |
| Für eine schnelle Verriegelung des PCs in Windows-Betriebssystemen genügt es, die Taste "Windows" + "L" gemeinsam zu drücken. |




Darüber hinaus ist es sinnvoll, eine **automatische PC-Sperre mit passwortgeschütztem Bildschirmschoner** für Minuten der Nichtbenutzung zu konfigurieren.

| Wichtig |
| --- |
| Bewahren Sie Ihre Passwort-Notizen niemals direkt an Ihrem Arbeitsplatz auf, z.B. unter der Schreibtischunterlage oder als Post-It auf dem Bildschirm! |


Damit kommen wir zum nächsten wichtigen Thema im Zusammenhang mit den Datenschutzmaßnahmen: Die korrekte Verwendung und sichere Handhabung von **Passwörtern**:

| Beispiel |
| --- |
| Die folgenden Passwörter sind sehr negative Beispiele, aber leider immer noch sehr beliebt:<br>• Kennwort1<br>• Vorname_Nachname_Geburtsdatum<br>• Nummernketten wie 123456<br>Sie sollten diese Passwörter niemals verwenden. Sie sind leicht zu hacken und daher sehr unsicher. |

Sind Sie besorgt, dass Ihre Passwortstärke schwach ist? Sie könnten Recht haben. Die folgenden Aspekte müssen bei der Erstellung eines starken Passworts beachtet werden:

| Hinweis |
| --- |
| • Länge des Passworts (mindestens 10 Zeichen)<br>• Eine Mischung aus Buchstaben und Zahlen, Sonderzeichen, Groß- und Kleinbuchstaben<br>• Keine Verwendung von Vor- oder Nachnamen, Geburtsdaten oder trivialen Passwörtern wie 123456 oder qwertz<br>• Ändern Sie Ihr Passwort in angemessenen Abständen<br>• Halten Sie Ihr Passwort stets geheim und senden Sie es nicht unverschlüsselt per E-Mail<br>• - Verwenden Sie private Login-Passwörter (z.B. für Facebook, Online-Kundenkonten) nicht für berufliche Zwecke. |

Co-funded by the
Erasmus+ Programme
of the European Union

# 7.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Das Unternehmen, für das Sie arbeiten, benötigt eine klare Schreibtisch-/Schirmpolitik. Was bedeutet das?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Sie sollten alle vertraulichen Dokumente sperren, wenn Sie nicht an Ihrem Schreibtisch sitzen.
- Sie sollten sich von Ihrem PC abmelden, wenn Sie Ihren Arbeitsbereich verlassen.
- Sie sollten nichts Unnötiges auf dem Desktop Ihres PCs speichern.
- Für eine schnelle Sperrung eines PCs mit Windows-Betriebssystem genügt es, die Tastenkombination "Windows-Taste" und "L" zu drücken.
- Private Dinge sollten Sie nicht auf Ihrem Arbeitstisch aufbewahren.

## Übung MULTIPLE CHOICE

Situation: Was sollten Sie bei der Wahl eines Passwortes beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Wenn Sie wahrscheinlich Ihr Passwort vergessen werden, notieren Sie sich ein Passwort, auf das Sie immer leicht zugreifen können (z.B. Post-it bei der Arbeit).
- Versuchen Sie, keine Sonderzeichen zu verwenden.
- Verwenden Sie nicht dasselbe Passwort für private und berufliche Zwecke.
- Achten Sie darauf, ein Passwort zu wählen, das lang genug ist.
- Ihr Vorname in Kombination mit Ihrem Familiennamen oder Ihrem Geburtsdatum sind relativ sichere Passwörter.

Co-funded by the
Erasmus+ Programme
of the European Union

# Quellen

jusline.at: https://www.jusline.at/gesetz/dsgvo

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

wko.at: https://www.wko.at/site/it-safe/kmu-handbuch.pdf

arbeiterkammer.at: https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/FAQ_DSGVO.pdf

dsb.gv.at: https://www.dsb.gv.at/documents/22758/116802/dsgvo_leitfaden.pdf/640015cb-eb90-4702-bf29-ca4fa2d32aca

wko.at: https://media.wko.at/epaper/Leitfaden-Sicherheitsmassnahmen-DSGVO/#20

wko.at: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/datenschutz-grundverordnung-fragen-und-antworten.html#heading_1__Bin_ich_von_der_DSGVO_betroffen_

wko.at: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-oesterreichisches-datenschutzgesetz.html

bmf.gv.at: https://www.bmf.gv.at/en/data-protection.html

gdpr.eu: https://gdpr.eu/eu-gdpr-personal-data/

gdpr-info.eu: https://gdpr-info.eu/

ico.org.uk: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf )

ec.euorpa.eu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

cyberthreatportal.com: https://cyberthreatportal.com/types-of-data-security-measures/

Co-funded by the
Erasmus+ Programme
of the European Union

# Wissen speichern

## Zusammenfassung

Der Begriff **Datenschutz** bezieht sich auf **den Schutz der Menschen** vor dem Missbrauch ihrer persönlichen Daten.

Der Schutz der persönlichen Daten natürlicher Personen ist auch das Hauptziel der Europäischen Allgemeinen Datenschutzverordnung (GDPR). Seit dem 25. Mai 2018 gilt die GDPR unmittelbar in jedem Mitgliedsstaat der EU und nationale Datenschutzbestimmungen haben nur ergänzenden Charakter.

Neben **neuen Definitionen** bringt das BIPR eine **Erweiterung der Rechte der Betroffenen**, eine Erhöhung der Datenbearbeitungspflichten und strengere Strafen für Datenschutzverletzungen mit sich. Die Umsetzung des GDPR wird von unabhängigen Aufsichtsbehörden in jedem Mitgliedsstaat überwacht.

Der objektive Anwendungsbereich des BIPR beschränkt sich auf die Verarbeitung von **Daten mit Personenbezug**. Das GDPR gilt nicht nur für maschinell verarbeitete Daten, sondern auch für manuell verarbeitete Daten, soweit diese Daten in einem Dateisystem gespeichert sind (oder gespeichert werden sollen).

Personenbezogene Daten im Sinne des GDPR sind alle Informationen über eine **bestimmte oder bestimmbare natürliche Person**. Sogenannte **sensible Daten** wie Daten zum Gesundheitszustand oder zur religiösen oder politischen Orientierung werden als besondere Datenkategorien behandelt. Neben der Einwilligung der betroffenen Person gibt es weitere Voraussetzungen für die rechtmäßige Verarbeitung nicht-sensibler Daten. Die Verarbeitung sensibler Daten ist nur in Ausnahmefällen zulässig.

Eine **gültige Einwilligungserklärung** muss freiwillig, für den spezifischen Verarbeitungszweck sowie in einer informierten und unmissverständlichen Weise abgegeben werden und kann jederzeit widerrufen werden.

**Die Grundsätze für eine GDPR-konforme Datenverarbeitung** sind Rechtmäßigkeit und Transparenz, Zweckbindung, Datenminimierung und -richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.

Sobald Personendaten verarbeitet werden sollen, muss die betroffene Person über bestimmte Aspekte der Datenverarbeitung **informiert werden**. Die Informationen müssen den betroffenen Personen in einer transparenten und leicht zugänglichen Form, in klarer und einfacher Sprache und kostenlos zur Verfügung gestellt werden.

Das GDPR verlangt Datenschutz durch Voreinstellungen (**privacy by default**) und datenschutzfreundliche Technikgestaltung (**privacy by desgin**).

Im Falle einer **Datenverletzung** sind, die für die Datenverarbeitung Verantwortlichen verpflichtet, die Datenschutzbehörde innerhalb von 72 Stunden zu benachrichtigen, wenn eine Gefährdung der Rechte und Freiheiten der betroffenen Personen nicht ausgeschlossen werden kann.

Die **Rechte der betroffenen Personen** sind im Rahmen des GDPR gestärkt worden. So muss Anträgen auf Zugang, Berichtigung, Löschung, Übertragbarkeit von Daten oder Einspruch gegen die Verarbeitung Beachtung geschenkt werden. Für die Beantwortung von Datenschutzanfragen und die Behandlung von Datenschutzbelangen der betroffenen Personen sind allein die für die Datenverarbeitung Verantwortlichen zuständig und befugt, die DatenverarbeiterInnen haben jedoch eine so genannte Unterstützungspflicht.

Co-funded by the
Erasmus+ Programme
of the European Union

Um die Daten ausreichend zu schützen, sind ein **Datenschutzkonzept** und die Einbeziehung von **geschultem Personal** notwendig. Darauf aufbauend können verschiedene Maßnahmen ergriffen werden, um Verstöße gegen Datenschutzgesetze und deren schwerwiegende Folgen zu verhindern.

Co-funded by the
Erasmus+ Programme
of the European Union

# Lösungsschlüssel
# (die korrekten Antworten sind fett markiert)

## 1.Wissen anwenden

### Übung MULTIPLE CHOICE

Situation: Worum geht es beim Begriff Datenschutz?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Der Datenschutz wird auch als Informationsschutz bezeichnet.**
- Beim Datenschutz geht es in erster Linie um den richtigen Umgang mit vertraulichen Unternehmensdaten und deren Schutz vor Missbrauch.
- **Datenschutz kann interpretiert werden als das Recht eines jeden Menschen, selbst zu entscheiden, wer, wann und in welchem Umfang Zugang zu personenbezogenen Daten hat.**
- Datenschutz hat nichts mit Datensicherheit zu tun.

### Übung SINGLE CHOICE

Situation: Datenschutz ist wichtig für welchen der folgenden Zwecke?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Der Datenschutz ist wichtig, damit die Banken bessere Kreditentscheidungen treffen können.
- **Der Datenschutz ist wichtig, damit die Menschen die Kontrolle über ihre persönlichen Daten behalten.**
- Der Datenschutz ist wichtig, damit Unternehmen ihre Marketingaktivitäten optimieren können.
- Datenschutz ist wichtig, damit Unternehmen überhaupt keine persönlichen Daten mehr verarbeiten dürfen.

### Übung MULTIPLE CHOICE

Situation: Was ist das GDPR und unter welchen Bedingungen gilt es?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Die GDPR ist eine europäische Verordnung, die in jedem europäischen Mitgliedsstaat direkt anwendbar ist.**
- Das GDPR ist eine europäische Verordnung, die von Mitgliedsstaaten, die kein eigenes nationales Datenschutzgesetz haben, freiwillig eingehalten werden kann.
- Das GDPR gilt für alle vertraulichen Unternehmensdaten, wie z.B. Betriebsgeheimnisse oder Preis- und Kostenkalkulationen.
- Das GDPR gilt nur für Unternehmen mit Sitz in einem europäischen Mitgliedsstaat und ist daher nicht auf Facebook, Google oder andere Großunternehmen mit Sitz in den USA anwendbar.
- **Ziel des GDPR ist es, die Rechte des Einzelnen zu stärken und das Datenschutzrecht in der EU zu harmonisieren.**

### Übung MULTIPLE CHOICE

Situation: Was versteht man unter einem Datenverarbeiter bzw. einer Datenverarbeiterin und was unter einem für die Datenverarbeitung Verantwortlichen bzw. einer für die Datenverarbeitung Verantwortlichen im Sinne des GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Ein/e für die Datenverarbeitung Verantwortliche/r entscheidet über den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten.**
- Ein/e DatenverarbeiterIn entscheidet über den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten.
- **Ein/e DatenverarbeiterIn verarbeitet Daten im Auftrag des für die Verarbeitung Verantwortlichen.**
- Die MitarbeiterInnen eines für die Datenverarbeitung Verantwortlichen bzw. einer für die Datenverarbeitung Verantwortlichen werden in der Regel als DatenverarbeiterIn betrachtet.
- Ein/e für die Datenverarbeitung Verantwortliche/r verarbeitet Daten im Auftrag des Datenverarbeiters bzw. der DatenverarbeiterIn.

## Übung SINGLE CHOICE

Situation: Die Österreicherin Josefa H. ist überzeugt, dass ihre Datenschutzrechte durch die deutsche Firma Easyshop verletzt worden sind. Welche der folgenden Aussagen sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

- Josefa H. muss sich an die Datenschutzbehörde in Deutschland wenden, um ihre Datenschutzrechte geltend zu machen, da Easyshop seinen Sitz in Deutschland hat.
- **Die Datenschutzbehörde kann bei schweren Datenschutzverletzungen hohe Strafen von bis zu 20 Millionen Euro verhängen.**
- Aufgrund der unterschiedlichen Rechtslage im Bereich des Datenschutzes in Österreich und Deutschland sollte Frau Josefa H. zunächst herausfinden, in welchem der beiden Länder ihre Datenschutzbeschwerde erfolgreicher sein könnte.
- Frau Josefa H. sollte sich auf jeden Fall einen Anwalt suchen, denn als Privatperson können Sie sich leider nicht an Datenaufsichtsbehörden wenden.

### 2.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle ist das GDPR anwendbar?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Eine Marketingfirma sammelt Namen und E-Mail-Adressen per Telefonanruf und speichert sie elektronisch.**
- **Ein kleiner Handwerksbetrieb führt eine Kundenliste (Namen und Telefonnummern) in Papierform.**
- Die Beamtin Lisa S. ist Mitglied einer nationalen Sicherheitsbehörde. Im Rahmen ihrer Tätigkeit wertet sie Telefonprotokolle aus.

- Peter P. ist kürzlich zum Geschäftsführer eines langjährigen Familienunternehmens befördert worden. Er will sich auf neue Geschäftsfelder konzentrieren und löscht deshalb zahlreiche Einträge aus der bestehenden Kundendatenbank.
- Die Studentin Sarah K. notiert sich die Kontaktdaten mehrerer Kommilitonen.
- Die Mitarbeiterin Maria S. wertet die Ergebnisse einer schriftlichen Kundenbefragung aus. Die Umfrage wurde mittels Fragebögen in Papierform durchgeführt. Die Kunden wurden gebeten, ihre Postleitzahl anzugeben, die Angabe ihres Namens war jedoch freiwillig.

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Daten sind personenbezogene Daten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Name einer Person
- Geburtsdatum
- Adresse einer Person
- Standort des Unternehmens
- Einkommen
- Verkaufszahlen
- Mitarbeiterfoto auf der Firmen-Homepage
- E-Mail-Adressen einer Person
- E-Mail-Adresse eines Unternehmens

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Daten sind sensible Daten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Fingerabdruck
- Anamnese
- Alter
- Angaben zum Konto
- sexuelle Orientierung

# 3.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Als MitarbeiterIn eines Beratungsunternehmens verarbeiten Sie verschiedene Kundendaten. Was sollten Sie beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Die Verarbeitung von Personendaten muss auf das unbedingt Notwendige beschränkt werden
- bestehende persönliche Daten dürfen nicht aktualisiert werden
- persönliche Daten dürfen nicht unbegrenzt gespeichert werden
- die Daten müssen vor unbefugter Verarbeitung geschützt werden

- **Höchststrafen werden wahrscheinlich im Falle eines Verstoßes gegen grundlegende Datenschutzprinzipien verhängt**

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle fällt die Verarbeitung personenbezogener, nicht-sensibler Daten unter eine der sechs Rechtsgrundlagen und ist daher zulässig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffend sein.

- **Ein Kunde bzw. eine Kundin kauft eine neue Küche und möchte sie zu sich nach Hause geliefert bekommen. Der Verkäufer bzw. die Verkäuferin notiert die Adresse der Kundschaft und speichert sie in der Kundendatenbank.**
- **In einem Unternehmen werden die Arbeitszeiten aller MitarbeiterInnen erfasst und verarbeitet.**
- **Ein Kunde bzw. eine Kundin stimmt der Verarbeitung seiner/ ihrer persönlichen Daten zu und unterzeichnet eine Einverständniserklärung.**
- Ein Sportverein veröffentlicht die Geburtsdaten der Neugeborenen seiner Mitglieder und deren Hochzeitsdaten in einer Vereinszeitung.

## Übung MULTIPLE CHOICE

Situation: Stellen Sie sich vor, Sie möchten personenbezogene Daten verarbeiten. Mangels anderer Rechtsgrundlagen benötigen Sie die Einverständniserklärung der betroffenen Personen. Was müssen Sie beachten?
Die Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Die Einwilligung kann von der betroffenen Person jederzeit zurückgezogen werden.**
- **Bei Personen, die das 16. Lebensjahr noch nicht vollendet haben, ist für eine gültige Einwilligung die Zustimmung eines Elternteils oder Erziehungsberechtigten erforderlich.**
- Die EU-Mitgliedstaaten können eine höhere Altersgrenze für die Einholung der elterlichen Zustimmung festlegen.
- **Die EU-Mitgliedsstaaten können eine niedrigere Altersgrenze für die Einholung der elterlichen Zustimmung festlegen.**

## Übung MULTIPLE CHOICE

Situation: In welchem der folgenden Fälle ist die Verarbeitung sensibler Daten erlaubt?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Eine bewusstlose Person wird nach einem Unfall ins Krankenhaus gebracht. Daten wie Blutgruppe, Alter oder Allergien werden verarbeitet.**
- **Eine homosexuelle Person spricht in einem Fernsehinterview offen über ihre sexuelle Orientierung.**
- In keinem der Fälle, da die Verarbeitung sensibler Daten ausnahmslos streng verboten ist.
- Die Verarbeitung sensibler Daten ist nur in einem Fall erlaubt, nämlich dann, wenn die betroffene Person ihre Einwilligung gibt.

## 4.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Was gilt als Datenverletzung im Sinne des GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Unbefugte Personen haben durch einen Hackerangriff Zugriff auf persönliche Daten erhalten.**
- **Ein Mitarbeiter bzw. eine Mitarbeiterin hat versehentlich zahlreiche Kundendaten gelöscht.**
- Ein Laptop mit wichtigen Aussagen über die neue Marketingstrategie des Unternehmens wurde gestohlen.
- **Ein Mitarbeiter bzw. eine Mitarbeiterin einer Personalagentur verlor einen USB-Stick, auf dem unter anderem zahlreiche Lebensläufe und Notizen zur persönlichen Situation von KundInnen gespeichert waren.**

## Übung MULTIPLE CHOICE

Situation: Bei einer Krankenkasse kam es zu einem Cyber-Angriff. Hacker haben sich Zugang zu zahlreichen Gesundheitsdaten der Versicherten verschafft. Wie ist das Vorgehen nach dem GDPR?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehrere oder alle Optionen können wahr sein.

- **Es besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, weshalb der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche die betroffene Person auch über diesen Vorfall informieren muss.**
- **Der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche muss die Datenschutzbehörde innerhalb von 72 Stunden informieren.**
- Der/ die DatenverarbeiterIn muss den für die Datenverarbeitung Verantwortlichen bzw. die für die Datenverarbeitung Verantwortliche innerhalb von 72 Stunden benachrichtigen.
- Der/ die DatenverarbeiterIn muss die Datenschutzbehörde innerhalb von 72 Stunden benachrichtigen.
- Da es sich nicht um sensible Daten handelt, reicht es aus, die Datenschutzbehörde zu benachrichtigen. Der für die Datenverarbeitung Verantwortliche bzw. die für die Datenverarbeitung Verantwortliche kann auf die Benachrichtigung der betroffenen Person verzichten.

## 5.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Mit dem GDPR werden die Rechte des Einzelnen gestärkt. Auf welche Rechte kann sich der Einzelne nun berufen?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Recht auf Einspruch**
- **Recht auf Information**
- Recht auf Veröffentlichung
- **Recht auf Datenportabilität**

- **Recht auf Berichtigung**
- **Recht auf Zugang**
- Recht auf gerechte Bezahlung für Daten

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen über das Recht auf Information und das Auskunftsrecht sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- **Das Auskunftsrecht gibt den betroffenen Personen das Recht, eine Kopie ihrer verarbeiteten** Personendaten zu erhalten.
- Das Recht auf Information ist genau dasselbe wie das Auskunftsrecht.
- **Das Auskunftsrecht bedeutet, dass die um Auskunft ersuchende Person auch das Recht hat, darüber informiert zu werden, dass keine sie betreffenden Personendaten bearbeitet werden (Negativinformation).**
- **Das Recht auf Information bedeutet, dass der/die für die Datenverarbeitung Verantwortliche die betroffenen Personen aktiv über bestimmte Punkte der Datenverarbeitung informieren muss.**

## Übung MULTIPLE CHOICE

Situation: Ein/e KundeIn kontaktiert Sie telefonisch. Er/ Sie möchte wissen, welche Daten von ihm/ ihr in Ihrem Unternehmen verarbeitet werden. Wie reagieren Sie darauf?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Ich beantworte seine Anfrage sofort.**
- Ich beantworte seine Anfrage, wenn ich die Kundschaft kenne und keine sensiblen Daten von ihm verarbeitet werden.
- Ich werde die Anfrage beantworten, wenn ich die Kundschaft kenne.
- **Ich teile der Person mit, dass ich persönlich als MitarbeiterIn ohne ausdrückliche Weisung keine Auskünfte erteilen darf und bitte, seine/ ihre Anfrage schriftlich an die Verantwortlichen für die Datenverarbeitung zu richten.**

## Übung MULTIPLE CHOICE

Situation: Wer ist laut DSGVO für die Beantwortung von Datenschutzanfragen von Betroffenen zuständig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehrere oder alle Optionen können wahr sein.

- BearbeiterIn der Daten
- **Verantwortliche für die Datenverarbeitung**
- Angestellte, wenn sie die betreffende Person zweifelsfrei identifizieren können
- Nur die Datenschutzbehörde

## Übung MULTIPLE CHOICE

Situation: Herr P. erhält seit einigen Wochen Postsendungen von einem Unternehmen, das ihm nicht bekannt ist. Er beschließt daher, dieses Unternehmen telefonisch um Auskunft darüber zu bitten, welche persönlichen Daten das Unternehmen über ihn hat und woher das Unternehmen diese Daten erhalten hat.
Welche der folgenden Aussagen ist richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- **Das Unternehmen kann Herrn P. um einen Identitätsnachweis bitten, bevor es auf sein Auskunftsersuchen antwortet.**
- **Wenn Herr P. innerhalb eines Monats keine Antwort oder Informationen vom Unternehmen erhält, kann er bei der Datenschutzbehörde eine Beschwerde einreichen.**
- Herr P. kann sein Auskunftsrecht nur persönlich vor Ort, gegen Vorlage eines Personalausweises, geltend machen.
- Das Unternehmen ist berechtigt, für die Übermittlung von Informationen in Papierform eine Gebühr zu verlangen. Lediglich die Übermittlung in elektronischer Form muss für den Auskunftsuchenden kostenfrei sein.

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Aussagen zum Recht auf Datenportabilität sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können zutreffen.

- **Einzelpersonen können die Übermittlung der personenbezogenen Daten, die sie einer für die Datenverarbeitung verantwortlichen Person zur Verfügung gestellt haben, beantragen.**
- **Das Recht gilt nur, wenn die Daten auf der Grundlage einer Einwilligung oder eines Vertrages verarbeitet werden.**
- Auch Unternehmen können das Recht auf Datenportabilität geltend machen.
- Das Recht auf Datenübertragbarkeit ermöglicht es Ihnen, Ihren derzeitigen E-Mail-Provider zu bitten, Ihre Kontaktliste an einen neuen E-Mail-Provider zu senden. Die Kosten der Datenübermittlung gehen zu Lasten des neuen E-Mail-Providers.
- **Die Nichteinhaltung dieses Rechts kann zu hohen Geldstrafen führen.**

## Übung MULTIPLE CHOICE

Situation: Klaus heiratete im vergangenen Jahr und stimmte zu, dass der Fotograf Hochzeitsfotos zu Werbezwecken auf seiner Firmenwebsite veröffentlichen darf. Heute ist Klaus geschieden und er ärgert sich darüber, dass durch die Eingabe seines Namens bei Google seine Hochzeitsfotos für jedermann sichtbar sind. Welche der folgenden Aussagen sind richtig?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehrere oder alle Optionen können wahr sein.

- **Er hat das Recht, seine Zustimmung zur Datenverarbeitung durch den Hochzeitsfotografen zu widerrufen.**
- **Er hat auch das Recht zu verlangen, dass seine im Internet veröffentlichten Fotos gelöscht werden.**
- **Klaus Ex-Frau Lisa ist ausgezogen. Sie hat das Recht, eine Korrektur ihrer Kundendaten zu verlangen (neue Adresse).**
- Das Recht, die Bearbeitung einzuschränken, erlaubt es den Hochzeitsfotografen, die Fotos weiterhin für Werbezwecke zu verwenden.

Co-funded by the
Erasmus+ Programme
of the European Union

## 6.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Was ist mit den Begriffen "privacy for design" und "privacy by default" gemeint?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Privacy by design steht für Datenschutz durch entsprechende Voreinstellungen.
- **Privacy by default steht für Privatsphäre durch geeignete Voreinstellungen.**
- **Privacy by design steht für Datenschutz durch Technologieentwicklung.**
- **Eine App ist so voreingestellt, dass persönliche Daten von anderen BenutzerInnen nicht eingesehen werden können. Dies ist ein Beispiel für Privacy by default.**
- In einem Softwareprogramm werden alle nicht unbedingt notwendigen Daten anonymisiert gespeichert. Dies ist ein Beispiel für den standardmäßigen Datenschutz.

## Übung MULTIPLE CHOICE

Situation: Was sind die wichtigen Schutzziele im Datenschutz?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Integrität**
- **Verfügbarkeit von Daten**
- Offener Datenzugang
- **Vertraulichkeit**
- Hohe Lagerdauer
- Daten-Transparenz

## Übung MULTIPLE CHOICE

Situation: Was ist mit dem Begriff TOM gemeint und wer ist nach dem GDPR für deren Umsetzung verantwortlich?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Die Abkürzung TOMs steht für technische und organisatorische Maßnahmen zum Datenschutz.**
- Das Kürzel TOMs steht für technisch zwingende Maßnahmen zum Datenschutz.
- **Die für die Datenverarbeitung Verantwortlichen und die DatenverarbeiterInnen sind für die Umsetzung geeigneter TOMs verantwortlich.**
- Die für die Datenverarbeitung Verantwortlichen sind für die Implementierung geeigneter TOMs verantwortlich.
- Die Datenschutzbehörde ist für die genauen Maßnahmen verantwortlich, die zum Schutz der persönlichen Daten getroffen werden müssen.
- **Die Schulung von MitarbeiterInnen ist ein Beispiel für die Umsetzung von Datenschutzbestimmungen.**
- **Automatische Back-ups oder Pseudonymisierung sind Beispiele für TOMs.**

## Übung MULTIPLE CHOICE

Situation: Welche der folgenden Maßnahmen können in der Praxis für den Datenschutz eingesetzt werden?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehrere oder alle Optionen können wahr sein.

- **Regelmäßige Sicherungen.**
- **Grundschulung zum Datenschutz für alle MitarbeiterInnen.**
- **Um Zugang zu Kundendaten zu erhalten, benötigen Sie ein Passwort und einen Benutzernamen.**
- Wenn möglich, werden KundInnen unter ihrem echten Namen und nicht unter einer BenutzerInnen-ID erfasst.
- So viele Daten wie möglich werden so lange wie technisch möglich gespeichert.

## 7.Wissen anwenden

## Übung MULTIPLE CHOICE

Situation: Das Unternehmen, für das Sie arbeiten, benötigt eine klare Schreibtisch-/Schirmpolitik. Was bedeutet das?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Sie sollten alle vertraulichen Dokumente sperren, wenn Sie nicht an Ihrem Schreibtisch sitzen.**
- **Sie sollten sich von Ihrem PC abmelden, wenn Sie Ihren Arbeitsbereich verlassen.**
- Sie sollten nichts Unnötiges auf dem Desktop Ihres PCs speichern.
- **Für eine schnelle Sperrung eines PCs mit Windows-Betriebssystem genügt es, die Tastenkombination "Windows-Taste" und "L" zu drücken.**
- Private Dinge sollten Sie nicht auf Ihrem Arbeitstisch aufbewahren.

## Übung MULTIPLE CHOICE

Situation: Was sollten Sie bei der Wahl eines Passwortes beachten?
Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Wenn Sie wahrscheinlich Ihr Passwort vergessen werden, notieren Sie sich ein Passwort, auf das Sie immer leicht zugreifen können (z.B. Post-it bei der Arbeit).
- Versuchen Sie, keine Sonderzeichen zu verwenden.
- **Verwenden Sie nicht dasselbe Passwort für private und berufliche Zwecke.**
- **Achten Sie darauf, ein Passwort zu wählen, das lang genug ist.**
- Ihr Vorname in Kombination mit Ihrem Familiennamen oder Ihrem Geburtsdatum sind relativ sichere Passwörter.