Datenschutz (AP1)

Grundlagen • Datenschutzmodelle • DSGVO — Cheatsheet für die Prüfung

BEGRIFFE & ABGRENZUNG

Datenschutz vs. IT-Sicherheit

Was ist was?

Datenschutz: Schutz personenbezogener Daten und Rechte der betroffenen Person. Fragt immer: „Darf ich das?"

IT-Sicherheit: Schutz von Systemen und Daten allgemein, auch ohne Personenbezug. Fragt: „Ist es geschützt?"

Überschneidung: TOMs wie Zugriffsschutz dienen oft beiden Zielen.

Prüfungsfalle: „Verschlüsselung = Datenschutz erledigt" ist falsch — braucht auch Rechtsgrundlage, Zweck und Informationspflichten.

DSGVO-GRUNDPRINZIP

DSGVO: Ziel, Logik, Grundgedanke

Verbot mit Erlaubnisvorbehalt

Verarbeitung personenbezogener Daten ist grundsätzlich verboten — außer, es gibt eine Rechtsgrundlage.

Rechtmäßigkeit & Transparenz

Jede Verarbeitung muss rechtmäßig, fair und für Betroffene nachvollziehbar sein.

Rechenschaftspflicht

Verantwortliche müssen Einhaltung der DSGVO nachweisen können — nicht nur „machen", sondern „begründen + dokumentieren".

Merksatz: Nicht nur „machen", sondern „begründen + dokumentieren".

ART. 4 DSGVO

Personenbezogene Daten erkennen

Definition (Art. 4 Nr. 1)

Personenbezogen = Information über identifizierte oder identifizierbare natürliche Person.

Typische Beispiele

- Name, E-Mail-Adresse, Telefonnummer
- Kundennummer, Personalnummer
- IP-Adresse (oft personenbeziehbar)
- Standortdaten, Online-Kennung, Cookie-ID

Wichtige Unterscheidung

Anonymisiert: Kein Personenbezug mehr → DSGVO nicht anwendbar

Pseudonymisiert: Personenbezug bleibt → DSGVO weiterhin anwendbar

Prüfungsfalle

„Pseudonymisiert = anonym" ist **falsch**!

Beispiel: Hash einer E-Mail-Adresse ist meist pseudonymisiert, nicht anonym. Solange die Person mit vertretbarem Aufwand identifizierbar bleibt, gilt die DSGVO.

ART. 4 NR. 2

Was ist „Verarbeitung"?

Verarbeitung umfasst jeden Vorgang mit personenbezogenen Daten: erheben, erfassen, organisieren, ordnen, speichern, anpassen, verändern, auslesen, abfragen, verwenden, offenlegen, übermitteln, verbreiten, abgleichen, verknüpfen, einschränken, löschen oder vernichten.

Prüfungsfalle: „Nur Speichern zählt" ist falsch. Schon das Erheben oder Ansehen von Daten ist Verarbeitung. **Mini-Check:** „Wer sieht was, wann, wozu, wie lange?"

ART. 5 DSGVO

Grundsätze der Verarbeitung

Die „6 Gebote" für jede Datenverarbeitung:

Rechtmäßigkeit, Fairness, Transparenz

Verarbeitung muss auf Rechtsgrundlage beruhen, fair sein und für Betroffene nachvollziehbar.

Zweckbindung

Daten nur für festgelegte, eindeutige und legitime Zwecke erheben und verarbeiten.

Datenminimierung

Nur die Daten erheben, die für den Zweck wirklich erforderlich sind.

Richtigkeit

Daten müssen sachlich richtig und aktuell sein; falsche Daten sind zu löschen/korrigieren.

Speicherbegrenzung

Daten nur so lange speichern, wie für den Zweck nötig — nicht „ewig".

Integrität & Vertraulichkeit

Angemessene Sicherheit durch TOMs (Technisch-Organisatorische Maßnahmen).

Plus: *Rechenschaftspflicht — Einhaltung muss nachweisbar sein.*

Merksatz: *Zweck klar, Daten schlank, Fristen fest, Schutz aktiv.*

ROLLEN

Verantwortlichkeiten: Wer ist wer?

1

Verantwortlicher

Entscheidet über Zwecke und Mittel der Verarbeitung. Trägt die Verantwortung für DSGVO-Compliance.

2

Auftragsverarbeiter

Verarbeitet Daten im Auftrag des Verantwortlichen (z. B. Cloud-Hosting, Lohnbüro). Braucht AV-Vertrag.

3

Empfänger

Erhält personenbezogene Daten (z. B. Versanddienstleister, Zahlungsdienstleister).

4

Gemeinsame Verantwortliche

Mehrere Stellen legen gemeinsam Zwecke und Mittel fest (z. B. gemeinsames Portal).

Prüfungsfalle

„Dienstleister = automatisch Auftragsverarbeiter" ist nicht immer richtig. Wenn der Dienstleister eigene Entscheidungen über Zwecke/Mittel trifft, ist er selbst Verantwortlicher.

Merksatz: Wer „Zweck + Wie" festlegt, trägt den Hut.

ART. 6 DSGVO

Rechtsgrundlagen für Verarbeitung

Sechs mögliche Rechtsgrundlagen — mindestens eine muss vorliegen:

01

Einwilligung

Freiwillige, informierte, eindeutige Zustimmung der betroffenen Person.

02

Vertrag / vorvertragliche Maßnahmen

Erforderlich zur Vertragserfüllung oder auf Anfrage vor Vertragsschluss.

03

Rechtliche Verpflichtung

Gesetz schreibt Verarbeitung vor (z. B. Aufbewahrungspflichten).

04

Lebenswichtige Interessen

Zum Schutz vitaler Interessen einer Person (selten in der Praxis).

05

Öffentliches Interesse / öffentliche Gewalt

Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt.

06

Berechtigtes Interesse

Interessenabwägung: eigenes Interesse überwiegt Rechte der Betroffenen (mit Begründung).

Prüfungsfalle: „Einwilligung ist immer am sichersten" stimmt nicht. Einwilligung muss freiwillig, widerrufbar und nachweisbar sein. **Beispiel:** Rechnungsversand basiert meist auf Vertrag/gesetzlicher Pflicht, nicht auf Einwilligung.

ART. 7 DSGVO

Einwilligung wirksam gestalten

Anforderungen an wirksame Einwilligung

- **Freiwillig:** Keine Kopplung an Leistung, echter Spielraum zur Entscheidung
- **Informiert:** Betroffene müssen wissen, wofür sie zustimmen
- **Eindeutig:** Aktive Handlung (z. B. Haken setzen), kein Opt-out vorab angekreuzt
- **Zweckgebunden:** Für jeden Zweck separate Einwilligung
- **Widerrufbar:** Jederzeit und so leicht wie Zustimmung selbst
- **Nachweisbar:** Verantwortlicher muss belegen können, dass Einwilligung vorlag

Typische Prüfungsfallen

Opt-out vorangekreuzt: Problematisch, weil nicht eindeutig aktive Zustimmung.

Kopplung an Leistung: Wenn Zugang zu Dienst von Einwilligung abhängt, ist diese häufig nicht freiwillig.

Keine Widerrufsmöglichkeit: Widerruf muss genauso leicht sein wie Zustimmung (z. B. Abmeldelink im Newsletter).

Merksatz: Einwilligung = „Ja, ich will" + „Ich kann jederzeit nein sagen".

ART. 9 & 10 DSGVO

Besondere Datenkategorien

Diese Daten sind extra sensibel und haben strengere Regeln:

Gesundheitsdaten

Krankmeldung, Arztbriefe, Fitnessdaten

Biometrische/genetische Daten

Fingerabdrück, Gesichtserkennung, DNA

Religion, Weltanschauung

Glaubensgemeinschaft, politische Meinung

Gewerkschaftszugehörigkeit

Mitgliedschaft in Gewerkschaften

Sexualleben/Orientierung

Sexuelle Orientierung, sexuelles Verhalten

Strafdaten (Art. 10)

Verurteilungen, Straftaten

Grundsatz: Verarbeitung verboten, außer spezielle Ausnahme nach Art. 9 Abs. 2 greift (z. B. ausdrückliche Einwilligung, Arbeitsrecht, Gesundheitsversorgung).

Prüfungsfalle: „Art. 6 als Rechtsgrundlage reicht" ist bei Art. 9-Daten falsch. Du brauchst zusätzlich eine Ausnahme nach Art. 9 Abs. 2. **Beispiel:** Attest im Betrieb → sensible Daten → strenge Zugriffsrechte + Zweckbindung.

ART. 13/14 DSGVO

Informationspflichten

Was Betroffene zum Zeitpunkt der Datenerhebung wissen müssen:

- **Verantwortlicher**
  Name, Kontakt, ggf. Datenschutzbeauftragter
- **Zwecke + Rechtsgrundlage**
  Wofür und auf welcher Basis werden Daten verarbeitet?
- **Empfänger/Kategorien**
  Wer bekommt die Daten (z. B. Dienstleister)?
- **Speicherdauer/Kriterien**
  Wie lange werden Daten aufbewahrt?
- **Betroffenenrechte**
  Auskunft, Löschung, Widerspruch etc. + Beschwerderecht bei Aufsichtsbehörde
- **Weitere Pflichtangaben**
  Drittlandtransfer, Profiling, Pflicht zur Bereitstellung (falls zutreffend)

Mini-Check

Wer? Verantwortlicher
Was? Welche Daten
Wozu? Zweck
Wie lange? Speicherdauer
Wohin? Empfänger
Welche Rechte? Auskunft, Löschung...

Prüfungsfalle: „Datenschutzhinweis irgendwo im Footer reicht" ist falsch. Er muss zum Zeitpunkt und im Kontext der Erhebung verfügbar sein.

KAPITEL 3 DSGVO

Betroffenenrechte im Überblick

Auskunft

Art. 15: Welche Daten, Zweck, Empfänger, Speicherdauer

Berichtigung

Art. 16: Falsche Daten korrigieren lassen

Löschung

Art. 17: „Recht auf Vergessenwerden" (Ausnahmen beachten)

Einschränkung

Art. 18: Verarbeitung vorübergehend blockieren

Datenübertragbarkeit (Art. 20)

Daten in strukturiertem Format erhalten und ggf. an anderen Verantwortlichen übermitteln.

Widerspruch (Art. 21)

Insbesondere gegen Verarbeitung aus berechtigtem Interesse oder Direktwerbung.

Automatisierte Entscheidung (Art. 22)

Kein Recht auf rein automatisierte Einzelfallentscheidung (inkl. Profiling) ohne menschliche Prüfung.

Frist: In der Regel muss der Verantwortliche binnen 1 Monat reagieren.

Prüfungsfalle: Löschung ist nicht immer möglich (z. B. bei Aufbewahrungspflichten). **Merksatz:** Rechte müssen „einfach ausübbar" sein — Prozesse dafür planen!

ART. 28 DSGVO

Auftragsverarbeitung (AV-Vertrag)

Wann ist ein AV-Vertrag Pflicht?

Sobald ein Dienstleister **im Auftrag** personenbezogene Daten verarbeitet, ist ein Auftragsverarbeitungsvertrag (AVV) erforderlich.

Pflichtinhalte des AVV (Art. 28 Abs. 3)

- Gegenstand, Dauer, Art und Zweck der Verarbeitung
- Art der Daten, Kategorien betroffener Personen
- Pflichten und Rechte des Verantwortlichen
- Weisungsbefugnis des Verantwortlichen
- TOMs (technisch-organisatorische Maßnahmen)
- Umgang mit Subunternehmern
- Unterstützung bei Betroffenenrechten, Meldepflichten
- Löschung/Rückgabe der Daten nach Vertragsende

Typisches Praxisbeispiel

Situation: Unternehmen nutzt Cloud-CRM, um Kundendaten zu speichern und zu verwalten.

Einordnung: Der Cloud-Anbieter verarbeitet die Daten im Auftrag → **Auftragsverarbeiter** → AVV erforderlich.

Prüfungsfalle: „Eine Geheimhaltungsvereinbarung (NDA) reicht" ist falsch. Der AVV hat spezifische Pflichtinhalte gemäß Art. 28 DSGVO.

ART. 32 DSGVO

TOMs: Sicherheit der Verarbeitung

Technisch-Organisatorische Maßnahmen (TOMs) müssen ein angemessenes Schutzniveau gewährleisten — abhängig von Risiko, Stand der Technik, Kosten und Art/Umfang/Zweck der Verarbeitung.

Verschlüsselung

Daten in Transit (TLS) und at Rest verschlüsseln.

Zugriffskontrolle

Rollenrechte, Least Privilege, Multi-Faktor-Authentifizierung (MFA).

Backup & Restore

Regelmäßige Backups und getestete Wiederherstellungsprozesse.

Logging & Monitoring

Protokollierung von Zugriffen und Änderungen, Anomalieerkennung.

Schulungen

Mitarbeiter regelmäßig zu Datenschutz und IT-Sicherheit schulen.

Netzwerksicherheit

Firewalls, IDS/IPS, Segmentierung sensibler Bereiche.

Ziel: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherstellen.

Prüfungsfalle: „Ein Passwort für alle" ist ein No-Go. **Mini-Tipp:** Rollenrechte + MFA + Backup-Test = schnelle Punkte in der Prüfung.

ART. 25 DSGVO

Privacy by Design & Default

Privacy by Design

Datenschutz muss schon bei der Planung und Entwicklung von Prozessen, Produkten und IT-Systemen berücksichtigt werden — nicht erst nachträglich „reingepatcht".

- Architektur und Prozesse datenschutzfreundlich gestalten
- Datenminimierung von Anfang an einplanen
- Risikoanalyse vor Produktivstart

Privacy by Default

Voreinstellungen müssen so gewählt sein, dass standardmäßig nur die für den jeweiligen Zweck notwendigen Daten verarbeitet werden.

- Restriktive Standardfreigaben
- Kurze Log-Aufbewahrungszeiten
- Tracker/Cookies standardmäßig deaktiviert

Praxisbeispiele

Softwareprojekt: Datenschutz-Anforderungen im Requirements Engineering verankern, DSFA durchführen, Privacy-Tests vor Go-Live.

Default-Einstellung: Nutzer sehen nach Registrierung nur für sie relevante Daten, nicht automatisch alle Inhalte.

Merksatz: „Später patchen wir Datenschutz rein" ist teuer und riskant. Default = „weniger Daten, weniger Sichtbarkeit".

ART. 30 DSGVO

Verzeichnis von Verarbeitungstätigkeiten (VVT)

Das VVT ist ein internes Register, das alle Verarbeitungstätigkeiten dokumentiert — Pflichtdokument für die Rechenschaftspflicht.

Was muss rein?

- Name und Kontakt Verantwortlicher
- Zwecke der Verarbeitung
- Kategorien betroffener Personen und Daten
- Kategorien von Empfängern
- Drittlandtransfers (falls zutreffend)
- Löschfristen (oder Kriterien)
- TOMs (allgemeine Beschreibung)

Warum wichtig?

Muss der Aufsichtsbehörde auf Anfrage vorgelegt werden. Zeigt, dass man die eigenen Verarbeitungen im Griff hat und Rechenschaftspflicht ernst nimmt.

Beispiel-Eintrag: „Newsletter-Versand" → Zweck: Marketing; Daten: E-Mail, Name; Rechtsgrundlage: Einwilligung (Art. 6 Abs. 1 lit. a); Anbieter: XY; Löschfrist: nach Widerruf/Abmeldung.

Prüfungsfalle: „Nur für große Unternehmen" ist missverständlich. In der Praxis wird ein VVT fast immer erwartet; Ausnahmen sind sehr eng (unter 250 Mitarbeiter UND keine regelmäßige Verarbeitung UND kein hohes Risiko).

ART. 35 DSGVO

Datenschutz-Folgenabschätzung (DSFA)

Wann ist eine DSFA Pflicht?

Bei **voraussichtlich hohem Risiko** für Rechte und Freiheiten der Betroffenen — insbesondere bei:

- Umfangreichem Tracking/Profiling
- Systematischer Videoüberwachung
- Automatisierten Entscheidungen mit rechtlicher/erheblicher Wirkung
- Verarbeitung sensibler Daten (Art. 9) im großen Stil

Prüfungsfalle: DSFA ist keine „nachträgliche Formalität". Sie muss **vor** Start der Verarbeitung durchgeführt werden.

Was muss eine DSFA enthalten?

1. **Beschreibung der Verarbeitung:** Zweck, Datenarten, Empfänger, Systeme
2. **Notwendigkeit & Verhältnismäßigkeit:** Warum ist die Verarbeitung erforderlich? Gibt es mildere Mittel?
3. **Risikobewertung:** Welche Risiken für Betroffene (Vertraulichkeit, Integrität, Verfügbarkeit)?
4. **Maßnahmen zur Risikominderung:** TOMs, Privacy by Design, Zugriffskontrollen etc.
5. **Ggf. Stellungnahme DSB:** Falls Datenschutzbeauftragter vorhanden

Merksatz: Neues riskantes Verfahren? Erst DSFA, dann Live.

ART. 33/34 DSGVO

Datenpanne: Die 72-Stunden-Regel

Was ist eine Datenpanne?

Verletzung des Schutzes personenbezogener Daten — z. B. unbefugter Zugriff, Verlust, Vernichtung, Veränderung oder Offenlegung.

Meldepflicht an Aufsichtsbehörde (Art. 33)

- **Frist:** Unverzüglich, möglichst binnen 72 Stunden nach **Bekanntwerden**
- **Voraussetzung:** Wenn ein Risiko für Rechte/Freiheiten besteht
- **Inhalt:** Art der Verletzung, Kategorien Betroffener/Daten, Folgen, ergriffene Maßnahmen

Benachrichtigung Betroffener (Art. 34)

Wenn die Datenpanne voraussichtlich ein **hohes Risiko** für die Betroffenen zur Folge hat, müssen diese unverzüglich informiert werden.

Intern: Incident Response

- Incident-Plan, klare Verantwortlichkeiten
- Logs sichern, Beweismittel dokumentieren
- Lessons Learned, Prozess anpassen

Prüfungsfalle: 72 Stunden ab **Bekanntwerden**, nicht ab Vorfall.
Beispiel: Laptop mit Kundendaten gestohlen → Risiko bewerten, ggf. melden + Betroffene informieren.

ART. 83 & 82 DSGVO

Sanktionen & Haftung

20M€

Maximales Bußgeld

Bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes (je nachdem, was höher ist).

2

Haftungsebenen

Behördliche Bußgelder UND zivilrechtlicher Schadenersatz durch Betroffene (materiell/immateriell).

Bußgelder (Art. 83)

Aufsichtsbehörden können bei Verstößen gegen die DSGVO Geldbußen verhängen. Die Höhe richtet sich nach Schwere, Dauer, Vorsatz/Fahrlässigkeit, Kooperation mit Behörde und bereits ergriffenen Maßnahmen.

- **Schwere Verstöße:** Mangelnde Rechtsgrundlage, Verstoß gegen Betroffenenrechte, fehlende DSFA bei Pflicht
- **Moderate Verstöße:** Unzureichende TOMs, fehlendes VVT, fehlende AVV

Schadenersatz (Art. 82)

Betroffene können Schadenersatz für materielle oder immaterielle Schäden verlangen, die ihnen durch DSGVO-Verstoß entstanden sind. Auch ohne finanziellen Schaden kann ein Anspruch bestehen (z. B. bei Kontrollverlust über eigene Daten).

Merksatz: Datenschutz ist Management-Thema, nicht nur IT. Compliance schützt vor empfindlichen Strafen und Reputationsverlust.

DATENSCHUTZMODELL

Standard-Datenschutzmodell (SDM)

Was ist das SDM?

Das **Standard-Datenschutzmodell** ist eine Methode deutscher Datenschutzbehörden, um DSGVO-Anforderungen systematisch in konkrete technische und organisatorische Maßnahmen (TOMs) zu übersetzen.

Wie funktioniert es?

SDM arbeitet mit **Gewährleistungszielen**, die eng an IT-Schutzzielen orientiert sind (Vertraulichkeit, Integrität, Verfügbarkeit) und zusätzlich datenschutzspezifische Ziele umfassen (z. B. Datenminimierung, Transparenz, Intervenierbarkeit, Nichtverkettung).

Für jede Verarbeitungstätigkeit werden Risiken bewertet und Maßnahmen abgeleitet, die diese Gewährleistungsziele erfüllen.

Nutzen in der Praxis

- Strukturierte Risiko- und Maßnahmenableitung für Prozesse und IT-Systeme
- Hilft, rechtliche Anforderungen (DSGVO) in konkrete technische/organisatorische Schritte zu übersetzen
- Unterstützt bei Dokumentation und Nachweispflicht (Rechenschaftspflicht)

Prüfungsfalle: SDM ist kein „Tool" oder Software, sondern eine Vorgehensweise/Denkmatrix. **Merksatz:** SDM hilft, Recht → Technik/Organisation zu übersetzen.

KAPITEL V DSGVO

Drittlandtransfer: Basics

Datenübermittlung in Länder außerhalb EU/EWR erfordert zusätzliche Garantien (Kapitel V) — neben den üblichen DSGVO-Anforderungen.

Angemessenheitsbeschluss

EU-Kommission stellt fest, dass Drittland angemessenes Schutzniveau hat (z. B. Schweiz, UK, Japan unter Auflagen). Dann ist Transfer erleichtert.

Standardvertragsklauseln (SCC)

Von EU-Kommission genehmigte Vertragsklauseln, die zwischen Verantwortlichem und Empfänger im Drittland geschlossen werden. Zusätzlich ggf. Zusatzmaßnahmen (ergänzende TOMs).

Binding Corporate Rules (BCR)

Interne Datenschutzvorschriften eines Konzerns, die von Aufsichtsbehörden genehmigt wurden. Erlauben konzerninternen Datentransfer.

Weitere Ausnahmen

Einwilligung, Vertragserfüllung, lebenswichtige Interessen, öffentliches Interesse — jedoch eng auszulegen (Art. 49).

Prüfungsfalle: „Kapitel V ist die Rechtsgrundlage" ist falsch. Kapitel V **ergänzt** die Rechtsgrundlage (z. B. Art. 6), du brauchst trotzdem eine Basis nach Art. 6 oder Art. 9. **Beispiel:** US-Cloud → Transfer prüfen + Garantien (SCC) + Info im Datenschutzhinweis.

PRAXISFÄLLE

Typische AP1-Situationen

Bewerberdaten

Zweck: Bewerbungsverfahren (Art. 6 Abs. 1 lit. b oder Art. 88 DSGVO i.V.m. nationalem Recht)

Fristen: Löschen nach Abschluss, außer Einwilligung für Talentpool

TOMs: Beschränkter Zugriff, sichere Aufbewahrung

Mitarbeiterdaten

Zweck: Lohn, Zeiterfassung, HR-Verwaltung, gesetzliche Aufbewahrung

Rechtsgrundlage: Vertrag (Art. 6 Abs. 1 lit. b) oder rechtliche Verpflichtung (Art. 6 Abs. 1 lit. c)

TOMs: Zugriff nur Need-to-know, Rollenrechte, verschlüsselte Speicherung

Logfiles

Zweck: IT-Sicherheit, Fehleranalyse (berechtigtes Interesse, Art. 6 Abs. 1 lit. f)

Datenminimierung: Nur nötige Daten protokollieren (z. B. gekürzte IP)

Fristen: Kurze Speicherdauer (z. B. 7–90 Tage je nach Zweck)

Newsletter

Rechtsgrundlage: Einwilligung (Art. 6 Abs. 1 lit. a), Double-Opt-in empfohlen

Nachweis: Zeitstempel, IP bei Anmeldung speichern

Abmeldelink: In jeder Mail, einfach und kostenlos nutzbar

Mini-Formel für jeden Fall: Zweck + Rechtsgrundlage + Frist + Empfänger + TOMs.

CHECKLISTE

Prüfungsfallen-Klassiker

Die häufigsten Stolpersteine in AP1-Prüfungen — sauber unterscheiden!

1 Anonym vs. Pseudonym

Anonym: Kein Personenbezug mehr → DSGVO nicht anwendbar
Pseudonym: Personenbezug bleibt → DSGVO gilt weiterhin

2 Verantwortlicher vs. Auftragsverarbeiter

Verantwortlicher: Entscheidet über Zwecke und Mittel
Auftragsverarbeiter: Verarbeitet im Auftrag, braucht AVV

3 Einwilligung: Anforderungen

Freiwillig + informiert + eindeutig + zweckgebunden + widerrufbar + nachweisbar

4 Betroffenenrechte: Frist & Prozesse

Antwort in der Regel binnen 1 Monat. Prozesse müssen „einfach ausübbar" sein.

5 Datenpanne: 72-Stunden-Regel

Meldung an Behörde binnen 72h nach **Bekanntwerden**, ggf. Benachrichtigung Betroffener bei hohem Risiko.

6 Dokumentation: VVT/AVV/DSFA

Rechenschaftspflicht greifbar machen durch Pflicht-Artefakte: Verzeichnis von Verarbeitungstätigkeiten, AV-Verträge, Datenschutz-Folgenabschätzungen.

Merksatz: DSGVO ist zu 50% Recht + zu 50% Dokumentation/Prozess. Häufigster Fehler: Begriffe nicht sauber trennen oder Pflicht-Artefakte vergessen.

MINI-QUIZ

Teste dein Wissen!

Die 6 Grundsätze aus Art. 5 DSGVO

Nenne alle sechs Grundsätze der Datenverarbeitung (Stichworte reichen).

Tipp: Rechtmäßigkeit, Fairness, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität & Vertraulichkeit + Rechenschaftspflicht

Verantwortlicher vs. Auftragsverarbeiter

Ordne zu: Gib je ein Praxisbeispiel für Verantwortlicher und Auftragsverarbeiter.

Tipp: Verantwortlicher = Unternehmen, das eigene CRM betreibt; Auftragsverarbeiter = Cloud-Hosting-Anbieter, der Daten im Auftrag speichert

Datenschutzhinweis: Pflichtinhalte

Welche 3 Inhalte MUSS ein Datenschutzhinweis mindestens enthalten?

Tipp: Wer (Verantwortlicher), Wozu (Zweck + Rechtsgrundlage), Welche Rechte (Auskunft, Löschung, Widerspruch...)

Anonymisierung vs. Pseudonymisierung

Was ist der Unterschied? Wann gilt die DSGVO?

Tipp: Anonymisiert = kein Personenbezug mehr (DSGVO nein); Pseudonymisiert = Personenbezug bleibt (DSGVO ja)

Du bist bereit für die Prüfung!

Dieses Cheatsheet hat dir die wichtigsten Grundlagen, Begriffe und Prüfungsfallen kompakt aufbereitet:

- DSGVO-Grundprinzipien und Begriffe (Art. 4, 5)
- Rollen, Rechtsgrundlagen und Einwilligung (Art. 6, 7)
- Besondere Datenkategorien (Art. 9, 10)
- Informationspflichten und Betroffenenrechte (Art. 13–22)
- TOMs, Privacy by Design & Default (Art. 25, 32)
- Auftragsverarbeitung, VVT, DSFA (Art. 28, 30, 35)
- Datenpannen, Sanktionen, Haftung (Art. 33, 34, 82, 83)
- SDM, Drittlandtransfer, Praxisfälle

Viel Erfolg! 🎓

Abschlussmotto

> „Datenschutz ist keine Bremse, sondern ein Fundament für Vertrauen."

Wenn du die Grundsätze verinnerlicht hast, kannst du jede Prüfungssituation meistern. Denk an: Zweck, Rechtsgrundlage, Dokumentation, TOMs.