7 Maßnahmen zur IT-Sicherheit und zum Datenschutz

7.2 DATENSCHUTZ *AP1-PRÜFUNGSVORBEREITUNG*

Datenschutz regelt den Umgang mit personenbezogenen Daten und ist ein fundamentales Recht in der EU. Anders als oft angenommen, geht es nicht primär um technische Sicherheit, sondern um rechtliche Grundlagen, Verarbeitungszwecke und die Rechte betroffener Personen. Die technische Sicherheit ist dabei ein wichtiger Teilaspekt, aber nicht der Kern des Datenschutzes.

Zentraler Merksatz: *Datenschutz = Recht + Zweck + Rechte (nicht nur Sicherheit)*

Datenschutzgesetze in der EU und Deutschland

Rechtlicher Rahmen

*Die **Datenschutz-Grundverordnung (DSGVO)** bildet seit Mai 2018 das Fundament des europäischen Datenschutzes. Sie gilt unmittelbar in allen EU-Mitgliedstaaten und schafft einheitliche Standards für die Verarbeitung personenbezogener Daten. Die DSGVO legt fest, wann und wie Unternehmen und Organisationen personenbezogene Daten erheben, speichern und nutzen dürfen.*

*Das **Bundesdatenschutzgesetz (BDSG)** ergänzt die DSGVO um nationale Regelungen. Es konkretisiert Öffnungsklauseln der DSGVO und regelt spezifische Bereiche wie Beschäftigtendatenschutz, Videoüberwachung oder die Datenverarbeitung durch öffentliche Stellen in Deutschland.*

Praxis-Merker

***DSGVO:** Das „Grundgesetz" des Datenschutzes in der EU – gilt direkt und unmittelbar*

***BDSG:** Deutsche Ergänzung mit nationalen Besonderheiten und Detailregelungen*

Arbeitsauftrag: Nenne drei konkrete Pflichten eines Unternehmens nach der DSGVO (ohne Paragrafen zu zitieren).

Personenbezogene Daten – Definition und Kategorien

Direkt identifizierend

- *Name und Vorname*
- *Postadresse*
- *Telefonnummer*
- *E-Mail-Adresse (meist)*
- *Kundennummer*
- *Personalausweisnummer*

Indirekt identifizierend

- *IP-Adresse*
- *MAC-Adresse*
- *Standortdaten*
- *Online-Kennungen*
- *Cookie-IDs*
- *Geräte-Identifikatoren*

Besonders schützenswert

- *Gesundheitsdaten*
- *Biometrische Daten*
- *Religiöse Überzeugung*
- *Politische Meinung*
- *Gewerkschaftszugehörigkeit*
- *Genetische Daten*

Definition: *Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Entscheidend ist, ob eine Person direkt oder indirekt bestimmt werden kann – auch durch Kombination mehrerer Daten.*

Prüfungsfalle: *Die Aussage „Das sind nur technische Daten" ist oft falsch. Logdateien können personenbezogen sein, wenn sie Benutzer-IDs, IP-Adressen und Zeitstempel kombinieren und damit Rückschlüsse auf Personen ermöglichen.*

Arbeitsauftrag: Markiere folgende Daten als personenbezogen (Ja/Nein) und begründe in einem Satz: IP-Adresse, MAC-Adresse, Servername, Tickettext „User kann nicht drucken", Inventarnummer Laptop.

IT-nahe Beispiele aus der Praxis

Im IT-Betrieb entstehen täglich zahlreiche personenbezogene Daten, die oft nicht auf den ersten Blick als solche erkannt werden. Das Verständnis dieser Datenströme ist essenziell für datenschutzkonformen IT-Support.

Ticketsystem

Jedes Support-Ticket enthält Name des Anfragers, Abteilung, Kontaktdaten und oft detaillierte Problembeschreibungen. Der Tickettext kann sensible Informationen über Arbeitsabläufe oder technische Probleme einzelner Mitarbeiter enthalten.

Status: Personenbezogen

Firewall & Proxy-Logs

Protokolle erfassen Client-IP-Adressen, Ziel-URLs, aufgerufene Websites, Zeitstempel und Datenvolumen. Diese Kombination ermöglicht die Zuordnung des Surfverhaltens zu einzelnen Nutzern oder Arbeitsplätzen.

Status: Personenbezogen

Active Directory

Benutzerkonten enthalten Login-Namen, Gruppenzugehörigkeiten, Login-Zeiten, letzte Kennwortänderung und Organisationseinheiten. Diese Metadaten bilden das komplette Nutzungsverhalten im Netzwerk ab.

Status: Personenbezogen

HR-Systeme

Personalverwaltungssysteme verarbeiten hochsensible Daten: Gehaltsinformationen, Krankheitstage, Urlaubsanträge, Beurteilungen und Vertragsdaten. Viele dieser Informationen gehören zu besonders schützenswerten Kategorien.

Status: Personenbezogen + teils besonders sensibel

Arbeitsauftrag: Nenne fünf Daten aus einem IT-Betrieb und ordne sie zu: „Stammdaten" versus „Bewegungsdaten" sowie „personenbezogen ja/nein".

Rechte der Betroffenen nach DSGVO

Die DSGVO gewährt betroffenen Personen umfassende Rechte gegenüber Unternehmen und Organisationen, die ihre Daten verarbeiten. Diese Rechte sind nicht verhandelbar, unterliegen aber bestimmten Ausnahmen.

Auskunftsrecht

Welche Daten werden gespeichert? Zu welchem Zweck? Woher stammen sie? An wen wurden sie weitergegeben?

Berichtigung

Unrichtige oder unvollständige Daten müssen korrigiert werden.

Löschung

„Recht auf Vergessenwerden" – wenn rechtliche Gründe vorliegen (nicht immer sofort möglich).

Einschränkung

Verarbeitung temporär begrenzen, z.B. während einer Prüfung der Rechtmäßigkeit.

Datenübertragbarkeit

Daten in strukturiertem, maschinenlesbarem Format erhalten (in bestimmten Fällen).

Widerspruchsrecht

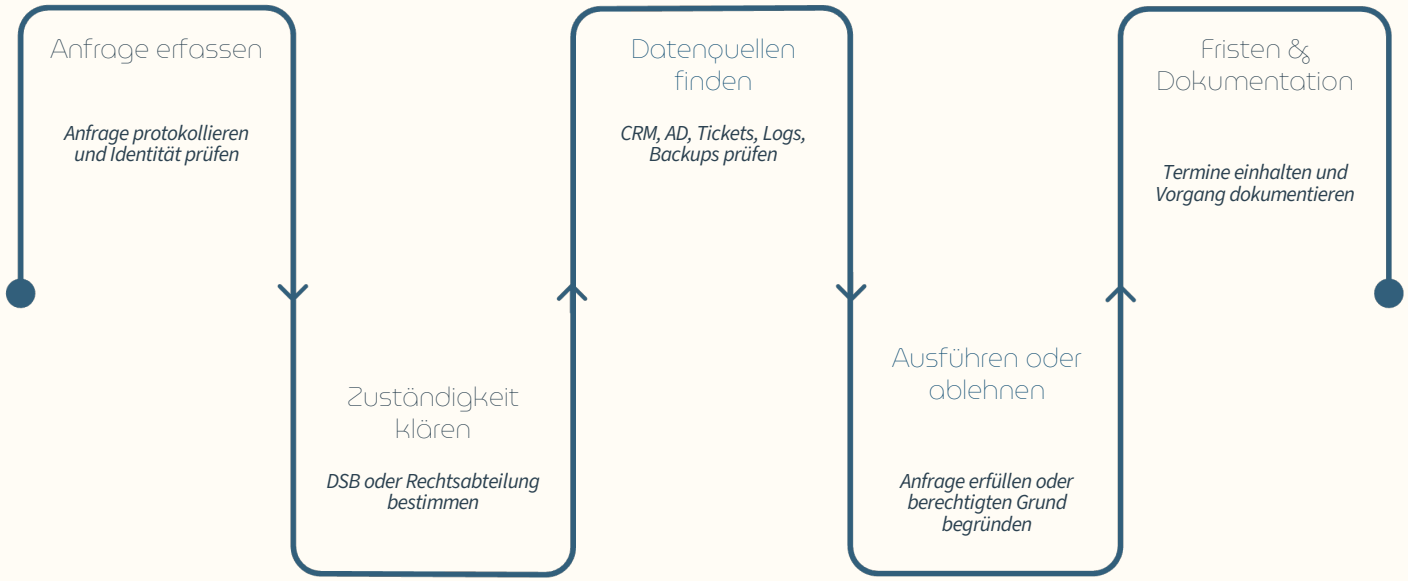
Gegen bestimmte Verarbeitungen widersprechen, insbesondere bei Direktwerbung.

Widerruf der Einwilligung

Erteilte Einwilligung jederzeit zurückziehen (für die Zukunft).

Prüfungsfalle: *Diese Rechte sind kein „Wunschkonzert". Es gibt gesetzliche Ausnahmen, etwa bei Aufbewahrungspflichten nach Handels- oder Steuerrecht. Eine sofortige Löschung ist dann*

Bearbeitung von Betroffenenanfragen im IT-Betrieb



Ohne ein strukturiertes Dateninventar wird die Bearbeitung von Betroffenenanfragen zum Chaos. IT-Abteilungen müssen wissen, wo welche personenbezogenen Daten gespeichert sind.

Kritische Erfolgsfaktoren

- ***Identitätsprüfung:*** *Sicherstellen, dass die anfragende Person tatsächlich berechtigt ist*
- ***Vollständigkeit:*** *Alle Systeme und Datenquellen systematisch prüfen*
- ***Fristen:*** *Grundsätzlich einen Monat Reaktionszeit (verlängerbar auf drei Monate bei Komplexität)*
- ***Dokumentation:*** *Jeden Schritt nachvollziehbar dokumentieren*
- ***Kommunikation:*** *Transparente und verständliche Antworten*

Typische Datenquellen

1. *Customer Relationship Management (CRM)*
2. *Active Directory / Verzeichnisdienste*
3. *Ticketsysteme und Support-Datenbanken*
4. *E-Mail-Archive und Mailserver*
5. *Logdateien (Firewall, Proxy, Webserver)*
6. *Backup-Systeme und Archivierungen*

Arbeitsauftrag: Ordne die folgenden sechs Beispielsätze dem passenden Betroffenenrecht zu: „Welche Daten habt ihr über mich gespeichert?" | „Meine Adresse ist falsch." | „Löscht mein altes Konto." | „Nutzt meine Daten nicht weiter, bis das geklärt ist." | „Gebt mir meine Daten als Datei." | „Ich will keine Werbemails mehr."

Mini-Prüfung: Datenschutz kompakt

AP1-PRÜFUNGSVORBEREITUNG

Teste dein Wissen mit diesen sechs prüfungsnahen Aufgaben. Sie decken die wichtigsten Kernthemen ab und entsprechen dem typischen AP1-Anforderungsniveau.

1

DSGVO vs. BDSG

Erkläre in einem Satz den wesentlichen Unterschied zwischen DSGVO und BDSG.

2

Definition

Definiere „personenbezogene Daten" in einem präzisen Satz.

3

IT-Praxisbeispiele

Nenne fünf konkrete Beispiele personenbezogener Daten aus IT-Logs oder Support-Tickets.

4

Betroffenenrechte

Zähle fünf verschiedene Rechte betroffener Personen nach DSGVO auf (Stichworte genügen).

5

IP-Adressen

Begründe in einem Satz, warum eine IP-Adresse häufig als personenbezogenes Datum gilt.

6

Prozessablauf

Skizziere einen 5-Schritt-Prozess zur Bearbeitung einer Auskunftsanfrage im IT-Betrieb.

> ***Erfolgstipp:*** *Datenschutz ist in der AP1-Prüfung kein theoretisches Wissen, sondern praktische Anwendung. Übe realistische Fallbeispiele und verknüpfe rechtliche Grundlagen mit IT-Prozessen.*