TB 4 - DSGVO & Datensicherheit

1. Datenschutz

Befasst sich mit dem Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten.

Verarbeitung von Daten wird immer umfangreicher. Große Unternehmen werden mit der EU-DSGVO 2016 streng reglementiert.

DSGVO

- Gilt seit 2018
- 99 Artikel
- 173 Erwägungsgründe
  - erklären, warum DSGVO wichtig ist
- 83 Öffnungsklauseln
  - geben Mindeststandards und Regelungen vor
  - fakultativ = können ausformuliert werden
  - obligatorisch = müssen ausformuliert werden

e-Privacy Verordnung

... eine veraltete Verordnung für Datenschutz in Österreich

Sachlicher Geltungsbereich

Personenbezogene Daten

... Daten die sich eindeutig auf eine natürliche Person beziehen oder diese identifizieren können (auch in einem bestimmten Kontext) z.B.: SV-Nummer, Fingerabdruck, Cookies, IP-Adresse

Für alle diese Daten gilt eine Sorgfaltspflicht

Wenn Daten (pseudo-)anonymisiert wurden, gilt DSGVO nicht

Verarbeitung

Manuelle oder (Teil-)automatisierte Bearbeitung von Daten in einem Dateisystem

Dateisystem

Strukturierte Speicherung von personenbezogenen Daten

Natürliche Personen

Ausnahmen

- persönliches/familiäres Umfeld
- nationale Sicherheit & Außenpolitik
- Strafverfolgung & Justiz

Räumlicher Geltungsbereich

DSGVO gilt für - Unternehmen, die in der EU niedergelassen sind - Unternehmen (aus Drittstaaten), die mit Daten von EU-Bürgern arbeiten - Unternehmen aus Drittsaaten ohne Niederlassung benötigen

Verantwortlicher

Jene Person die Daten erhebt und über Zwecke und Mittel der Verarbeitung verfügt. Muss eine rechtliche Grundlage für Verarbeitung nennen

Auftragsverarbeiter

Kann im Namen des Verantwortlichen den technischen Aspekt der Verarbeitung übernimmt.

Grundsätze der DSGVO

1. Rechtmäßigkeit, Treu und Glaube & Transparenz
   - **rechtmäßigkeit**
     - rechtliche Verpflichtung (z.B. Bank)
     - zur Erfüllung eines Vertrages
     - persönliche Einwilligung des Betroffenen
     - Wahrung lebenswichtiger Interessen
     - Aufgabe im öffentliche Interesse
     - berechtigtes Interesse
   - Treu und Glaube
     - Daten dürfen nicht in böswilligem Interesse erhoben werden
   - Transparenz
2. Zweckbindung
   - muss an bestimmten Zweck gebunden sein
   - wenn Zweck entfällt, muss erneut Einwilligung erhoben werden
3. Datenminimierung
   - nur notwendige Daten erheben
4. Richtigkeit
   - Daten müssen jederzeit richtig und aktuell sein
5. Speicherbegrenzung
   - Daten dürfen nur so lange gespeichert werden, wie notwendig

Einwilligung

- muss freiwillig sein
- jederzeit widerrufbar
- einfach und klar formuliert
- muss sich auf konkrete Verarbeitung beziehen

Besondere Kategorien von Daten

... dürfen grundsätzlich gar nicht erhoben werden, außer bei bestimmten Ausnahmen.

- Biometrische Daten
- politische Meinungen
- sexuelle Orientierung
- Ethnische Herkunft
- Gesundheitsdaten

Rechte von Betroffenen

- Auskunft
  - Verarbeiter muss auf Anfrage umgehend (1 Monat) antworten
  - Sanktionierung bis 20.000.000 € oder 4 % des Umsatzes
  - welche Daten
  - welcher Zweck
  - wie lange (Löschungsfristen)
  - so ziemlich, alles was im Verarbeitungsverzeichnis steht
- Berichtigung
- Löschung
  - immer dann, wenn Daten unrechtmäßig verarbeitet werden
- Einschränkung der Verarbeitung
  - Umfang der Verarbeitung einschränken
  - keine weiterführende Verarbeitung zulassen
  - Daten einfrieren
- Datenübertragbarkeit
  - Daten müssen von einem Anbieter auf anderen übertragbar sein
- Widerspruch
  - z.B. bei Direktwerbung sofort

Pflichten Verantwortlicher & Auftragsverarbeiter

- Betroffenenrechte erfüllen
- Verarbeitungsverzeichnis führen
- Technische & organisatorische Maßnahmen durchführen
- Datenschutzverletzungen melden
- DS-Risikoeinschätzungen durchführen
- DS-Bauftragten bestellen

- Mit DSB zusammenarbeiten

Verarbeitungsverzeichnis

- jede Verarbeitung auflisten
  - Zweck
  - Betroffenenkategorie
  - Technische & organisatorische Datensicherheitsmaßnahmen
  - Kategorien an Daten
  - Übermittlung (an Dritte? an Nicht-EU-Staaten?)
  - Löschungsfristen

Technische & organisatorische Maßnahmen

Informationssicherheitsziele einhalten

Maßnahmen müssen

- technisch aktuell sein
- verhältnismäßig sein
- dokumentiert sein (im Verarbeitungsverzeichnis)

Privacy by Design

Bei Systementwurf, Konzeption & Entwicklung Hauptaugenmerk auf Datensicherheit gelegt wurde.

- Datenminimierung
- Anonymisierung
- Pseudoanonymisierung

Privacy by Default

Voreinstellungen der Plattform erheben nur so viele Daten, wie mindest notwendig. Zusätzliche Datenerhebung muss von Betroffenen explizit zugestimmt werden

Datenschutzverletzungen

- Meldepflichtig wenn
  - physischer, materieller oder immaterieller Schaden erfolgt ist
  - dieser Schaden ein hohes Risiko für Betroffene darstellt

Datenschutzverletzungen liegen von, wenn:

- Verlust von Kontrolle über Daten
- Identitätsdiebstahl
- Verlust der Rechte
- finanzielle Verluste

- Verlust der Vertraulichkeit
- unbefugte Aufhebung von Pseudoanonymisierung

Ablauf

1. Datenleck liegt vor
2. Erkennen
3. Datenleck schließen
4. Konsequenzen für Betroffene abschätzen
5. Folgeschäden minimieren
6. Information der Betroffenen
7. Information DSB
8. Schadensbeseitigung
9. Analyse des Hergangs der Datenpanne
10. Präventive Maßnahmen umsetzen

Datenschutzfolgeabschätzung

- DSB gibt Black & Whitelist vor, die bestimmen, welche Verarbeitungen keine DSFA benötigen
- zwingend bei
  - systematische Bewertung persönlicher Aspekte von Betroffenen (Profiling)
  - umfangreiche Verarbeitung von sensiblen Daten
  - systematische Überwachung öffentlicher Bereiche

Inhalt

- Verarbeitungsvorgänge beschreiben
- Zwecke
- Daten & Aufbewahrung der Daten kritisch hinterfragen
- Risiken
- Eintrittwahrscheinlichkeit
- Schadensausmaß
- Präventive Maßnahmen zur Risikominderung

Datenschutzbeauftragter

- sämtliche Bestimmungen der DSGVO einhalten
- Beratung von Mitarbeitern
- Umsetzung von Maßnahmen
- Reporting ans Management
- ...

Zertifizierungen

- European Privacy Seal

  - 2-jährige Rezertifizierung
- Interessenvertretungen können Codes of Conduct vorgeben

Datenübermittlung ans Ausland

immer, wenn Daten ins EU-Ausland übermittelt werden, müssen EU-Bestimmungen eingehalten werden. Es kann mehrere Sicherstellungen geben:

Angemessenheitsbeschlüsse

- werden von der EU-Kommission erteilt
- gelten 4 Jahre lang
- z.B. UK, Japan, Uruguay, Kanada

Safe-Harbor Abkommen & US-EU-Privacy-Shield

- sind Abkommen für den Datenaustausch mit den USA
- mittlerweile nicht mehr gültig
- das EU-US-Privacy-Shield ist seit 2020 nicht mehr gültig

Geeignete Garantien

wenn ein Drittstaat keine Angemessenheitsbeschlüssen

- Binding Coorporate Rules
  - einmal von DSB genehmigt
- Standarddatenschutzklauseln
  - Verantwortliche
  - Auftragsverarbeiter
- genehmigt Verhaltensregeln (Codes of Conduct)
- sonst
  - separates Vertragswerk und im Einzelfall genehmigen lassen

DSB - Datenschutzbehörde

- Öffentlichkeit Informieren
- Anlaufstelle
- Hilfestellung
- Vorgaben erstellen (Black/White-List)

One-Stop-Shop-Prinzip

- bei Zusammenarbeit von Behörden mehrerer EU-Staaten
- Koherenzverfahren
- im Zweifelsfall hat EU-Datenschutzausschuss Entscheidung

2. Informationssicherheit

"Data is the new oil"

Bedrohungen

- Identitätsdiebstahl durch Phishing
- Ransomware
- Denial of Service
- Social Engineering
- Fehler von Personal
- Naturkatastrophen
- Advanced Persistent Threads

Gründe

- Wettbewerbsvorteil
- Compliance
  - Gesetze und Regelungen erfüllen (z.B. DSGVO, Telekommunikationsgesetz, e-Privacy Richtlinie)

Schutzziele nach ISO 27001

- Vertraulichkeit
  - Informationen für nicht authorisierte Personen unzugänglich
- Integrität
  - Information nicht gefälscht werden kann
- Verfügbarkeit
  - der Zugang zu Informationen wird nicht beeinträchtigt
  - Informationen sind nutzbar
  - kein Denial of Service, ...
- Authentizität
  - Echtheit einer Person prüfen
  - Man-in-the-Middle verhindern
  - 3 Stufen
    - Authentisierung = Credentials, ID, etc. herzeigen
    - Authensierung = Credentials, etc. prüfen
    - Authorisierung = Rechte zuweisen
- Zugriffssteuerung
  - Zugang zu bestimmten Informationen steuern
- Verlässlich
  - wenn Funktion aufgerufen wird immer gleich Ergebnisse
  - kein unvorhergesehenes Verhalten
- Verbindlichkeit
  - Genau feststellen wer was gemacht hat
  - geschützte Protokollierung

- Zurechenbarkeit
  - Ereignisse/Aktionen sind eindeutig einer Person zurechenbar
  - Eine Person ist für seine Aktionen verantwortlich

Standards

- ISO 27000
- BSI-IT Grundschutz
- NIST SP 800-xx
- ITIL
- ...

3. BSI-IT Grundschutz

Definiert, wie man Informationssicherheit schrittweise in einem Unternehmen einführen, entwickeln, implementieren kann.

ISO 27000 kann weiterführend umgesetzt werden

4 Standards

- Managementsysteme
- Vorgehensweise
- Risikoanalyse
- Notfallmanagement

Schutzniveaus

- Basis Schutzbedarf = Basis-Absicherung
  - ganz am Anfang
  - wenige Systeme mit hohem Schutzbedarf
- normaler Schutzbedarf = Standard-Absicherung
  - erst wenn Grundschutz schon implementiert wurde
  - auch weniger wichtige Aspekte der IT absichern
  - keine besondere Abgrenzung von zu schützenswerten Assets
- erhöhter Schutzbedarf = Kern-Absicherung
  - ganz am Anfang
  - nur für, einzelne besonders zu schützende Elemente der IT

Umsetzung

- Verfolgt einen ganzheitlichen Ansatz der Prozesse, Systeme, Personal, Ressourcen, ... umfasst
- PDCA

Prozess

- Initiierung
  - Grobkonzept
- Information Security Policy (Leitlinie) erstellen
- Organisation definieren
  - Verantwortlichkeiten
  - Ressourcen
- Sicherheitskonzeption erstellen
  - Feinkonzept
  - Bausteine auswählen
  - IT-Grundschutz Check
    - SOLL/IST-Vergleich
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

Initiierung

- Führung überzeugen
- Ressourcen freigeben
- Verantwortung übernehmen
  - ISB/CISO beauftragen
- Überblick IT-System
  - IST
  - Risiken
  - **Business Impact Analyse** = welche Folgen/Schäden hat der Ausfall eines IT-Systems => Maßnahmen definieren
- Schutzniveaus definieren

Leitlinie (Security-Policy) erstellen

- Leitlinie für Verhalten
- Commitment von Führung
- Längerfristige Strategie

Organisation

- Aufbauorganisation
- Verantwortlichkeiten
- ISB einbinden
- ISB & DSB zusammenarbeiten

Sicherheitskonzept erstellen

1. Strukturanalyse
   - GP, Anwendungen, Systeme, Schnittstellen, Infrastruktur erfassen
2. Schutzbedarfsfeststellung

- welchen Schutzbedarf haben einzelne Bestandteile meines Systems
- Arten
  - normal = Standard-Absicherung
    - bis 50.000 €
  - hoch = Standard-Absicherung + Risikoanalyse
    - bis 500.000 €
  - sehr hoch
    - über 500.000 €
- Prinzipien
  - Maximalprinzip = Server hat mindestens den Schutzbedarf seiner wichtigsten Anwendung
  - Kumulationsprinzip = Server hat höheren Schutzbedarf als seine, Anwendung, da gesamter Ausfall schlimmer wäre
  - Verteilungseffekt = durch redundante Ausführung des Servers kann Schutzbedarf verringert werden
- Sicherheitszonen
  - Räumlich
  - Technisch
  - Personell

3. Modellierung
   - Bausteine auswählen
   - Entwicklungskonzept oder Prüfplan als Resultat
4. IT-Grundschutz Check
   - Realisierung der Anforderungen prüfen
   - SOLL-IST-Vergleich
5. Risikoanalyse
   - implizit
     - bei Standard-Absicherung durchgeführt
     - bei Bausteinen inkludiert
   - explizit
     - bei hohem, sehr hohen Schutzbedarf
     - weitere Bedrohungen identifizieren und analysieren
     - Eintrittswahrscheinlichkeit
     - Schadensausmaß
     - Maßnahmen gegen Bedrohung

Umsetzung

- Sicherheitsmaßnahmen zusammenstellen
- Kosten/Aufwand vergleichen
- über Ressourcen entscheiden
- Termine
- Implementierung überwachen

Aufrechterhaltung und Verbesserung

- Überprüfung der Prozesse, Systeme
  - Kennzahlen
  - Dokumentation
  - Szenarien simulieren
  - Audits
- Aktualität prüfen
- Vorgehensweise erweitern

ISB

- Umsetzung von IS
  - Standards
  - Tools
  - Bedrohungen
- Business Impact Analyse
- Vorfälle analysieren
- Schulungen
- ...

Grundschutzkompendium

Enthält wichtige Elemente eines IT-Systems, abgebildet als Bausteine

Bausteine

Beschreibt eine bestimmte Komponente eines IT-Systems

Systembausteine = behandeln die einzelnen Komponenten des Systems

Prozessbausteine = behandeln die Abläufe und Prozesse in dem System

Struktur:

- Beschreibung
- Ziele
- Abgrenzung
- Gefährdungen
- Anforderungen
- Reihenfolge
- ...

Notfallmanagement

- wenn ein Notfall eintritt
  - wie verhalten
  - Szenario was im Normalbetrieb nicht bewältigt werden kann
- Business Impact

  - Ausfallzeiten
  - Recovery Time Objective
  - Recovery Point Objective
- Notfallhandbuch
  - Leitlinie für Notfall
  - Verantwortung
  - Kompetenzen
  - Kommunikation
  - Reihenfolge

4. BigData

erhöhte Datenmengen und Verarbeitungsgeschwindigkeiten, sodass klassische relationale Datenbanksysteme nicht mehr ausreichen

Datenmenge verdoppelt sich alle 2 Jahre

Daten liegen immer mehr unstrukturiert vor

Daten haben immer mehr betriebswirtschaftlichen Wert

Einsatzfelder

- Marketing
- Business Intelligente
- Finanzprüfung (Fraud-Detection)
- Medizin
- ...

V-Modell

- Volume
  - Moore-Theorem besagt, dass sich die Datenmenge pro Jahr verdoppelt (aktuell im Petabyte Bereich)
- Velocity
  - immer mehr Echtzeitberechnung
  - weniger Batch-Betrieb
  - Smartphones, Autos ...
- Variety
  - Daten liegen in immer unterschiedlicherer Form vor
- (Value)
  - Daten haben einen immer mehr betriebswirtschaftlichen Wert
- (Veracity)
  - Daten sind immer mehr strukturiert

Daten

Strukturiert

Daten die in relationalen DB gespeichert werden. Bei BigData kann es unter der Verwendung von herkömmlichen DBMS zu hohen Lizenzkosten kommen. Viele BigData-Systeme sind Open-Source.

Unstrukturierte Daten

können nicht konventionell gespeichert werden z.B. Bilder, Videos, ...

Semistrukturierte Daten

XML

Verarbeitung

Stream-Verarbeitung

Daten werden kontinuierlich in einem Stream verarbeitet (Echtzeitverarbeitung). z.B. Sensordaten aus Autos, Smartphones, ...

Batch-Verarbeitung

Daten werden in einem Stück verarbeitet (Batch-Verarbeitung). z.B. Daten aus einer Datenbank, Spreadsheets, ...

Speichersysteme

Hadoop File System

Dateien sind in Blöcken auf mehreren Nodes redundant gespeichert Name Node (auch redundant vorhanden) verwaltet Metadaten. Wenn Daten geschrieben werden, werden diese automatisch repliziert.

NoSQL

- Daten werden nicht normalisiert
- Skalierbarkeit
- Performance
- ACID-Prinzipien verletzt

Schichten

- Datenquellen
  - operative Systeme
  - Sensordaten
- Datenspeicherung
  - nicht-relationale Systeme (NoSQL)
  - Hadoop, MongoDB, ...

- Datenverarbeitung
- Ausgabe
  - Reports, Diagramme, ...
  - Decision-Support-Systems

Map-Reduce

Aufbereitung auf mehrere Knoten verteilen

Phasen

- Map (Parallel)
  - Daten werden in Chunks auf mehrere Nodes verteilt
- Shuffle & Sort
  - Die Werte von Schlüsseln/Attributen werden in (Wert-)Listen gespeichert
  - Die Schlüssel/Attribute werden nach ihrem Wert sortiert
- Reduce (Parallel)
  - Die Wertlisten werden zusammengeführt und aggregiert

CAP-Theorem

Ein verteiltes DBMS nicht alle drei Garantien erfüllen kann - Consistency - Daten werden sind trotz Mehrbenutzerbetrieb konsistent - Transactions überführen System von einem konsistenten Zustand zu einem anderen konsistenten Zustand - Jeder sieht dieselben Daten - Availability - Daten sind trotz Mehrbenutzerbetrieb immer verfügbar - Jeder kann lesen und schreiben - Partition Tolerance - System funktioniert auch verteilt

ACID

- Atomicity
  - Transaktionen sind atomar
- Consistency
  - Transaktionen überführen System von einem konsistenten Zustand zu einem anderen konsistenten Zustand
- Isolation
  - Transaktionen sind isoliert und beeinflussen einander nicht
- Durability
  - Datenänderungen sind von Dauer
  - keine unvorhergesehenen Datenverluste