4 EU-GDPR – Introduction

ISO 27001, A.18 

18.1 Compliance mit Gesetzen und vertraglichen Anforderungen

Ziel: Vermeidung von Verstößen gegen Gesetze, Verträge in Bezug auf Informationssicherheit.

18.2 IT Sec Überprüfungen

Ziel: Sicherstellen, dass IT Security im Einklang mit den Unternehmensrichtlinien und Prozeduren implementiert und angewendet wird

BSI 200,8 Compliance

Auswählen von Sicherheitsmaßnahmen

Compliance und Datenschutz

Grundsätze Datenschutz:

- Es geht um den Schutz der hinter den Daten stehenden Personen und nicht um die Daten als solche (Möglichkeit der Identifizierung reicht aus)
- Zu Datenschutz gehört auch IT-Sicherheit
- Jeder Bürger hat Grundrecht auf informationelle Selbstbestimmung
- "Verbot mit Erlaubnisvorbehalt" → Datenverarbeitung grundsätzlich verboten, es sei denn, es liegt eine rechtliche Legitimation vor.

Verarbeitung persönlicher Daten nach Ländern

Land/Region	**Gesetz**	**Vergleich EU-GDPR**
EU	EU-GDPR	
China	Personal Information Pretection Law (PIPL)	
Turkey	Turkey Data Protection Law	Wie GDPR
Brazil	Brazil Data Protection Law	Wie GDPR
Russia	~~Thai Personal Data Protection Act~~	
USA		
Mexico	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	

GDPR Territorialer Scope

- Data Subject: identifizierte oder identifizierbare natürliche Person
- Data Controller: natürliche oder legale Person mit dem Ziel persönliche Daten zu Erheben
- Data Processor: natürliche oder legale Person, die Daten für den Processor verarbeitet

Art. 3 Räumlicher Anwendungsbereich der DSGVO

- Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter mit Niederlassung in der EU.
- Verarbeitung personenbezogener Daten von Personen in der EU durch Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der EU, wenn:
    - Waren oder Dienstleistungen an Personen in der EU angeboten werden.
    - Das Verhalten von Personen in der EU beobachtet wird.
- Verarbeitung personenbezogener Daten durch Verantwortliche, die nicht in der EU niedergelassen sind, aber an einem Ort tätig sind, der dem Recht eines EU-Mitgliedstaats unterliegt.

Art. 4 DSGVO Definitionen

1. Persönliche Daten: alle Daten, die sich auf eine identifizierbare Person beziehen. Identifizierbar insofern, dass über Kennungen Rückschlüsse auf die natürliche Person gezogen werden können
2. Verarbeitung: Jeder Vorgang der auf personenbezogene Daten angewendet wird (Sammeln, Aufnehmen, Organisieren, Strukturieren, Speichern)
3. Pseudonymisierung: Verarbeitung personenbezogener Daten in einer Weise, dass diese nicht Rückschlüsse auf eine Person geben
4. Dateisystem: jede strukturierte Sammlung von personenbezogenen Daten, die nach Kriterien zugänglich sind
5. Controller: eine natürliche oder legale Person, die Daten mit dem Zweck erhebt, dass diese danach durch einen Processor verarbeitet werden
6. Processor: eine natürliche oder legale Person, die Daten im Auftrag des Controllers verarbeitet

GDPR Art. 5 Grundsätze bei der Verarbeitung personenbezogener Daten

Erhobene Daten sollten:

1. gesetzeskonform, zweckgemäß und transparent verarbeitet werden
2. nur für einen bestimmen Zweck erhoben werden
3. adäquat und minimal gehalten werden
4. genau und aktuell gehalten werden
5. nicht länger als nötig gespeichert werden
6. sicher gespeichert werden

Controller sind für die Einhaltung der Compliance zuständig

GDPR Art. 6 Rechtmäßigkeit der Erhebung

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung gegeben
- Vertragliche Notwendigkeit: wenn Daten verarbeitet werden müssen, um einen Vertrag/Dienstleistung zu erfüllen

- Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt
- die Verarbeitung ist zur Wahrung dem berechtigten Interesse des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person eingeschränkt werden

GDPR Art. 7 Bedingungen für die Einwilligung

Die Einwilligung muss unter folgenden Bedingungen erfolgen:

- Wenn auf Basis von Einwilligung, muss der Verantwortliche nachweisen, dass Person eingewilligt hat
- Einwilligung und Zweck muss klar und in verständlicher Sprache formuliert sein
- Die Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.
- Es muss nachgewiesen werden, dass die Einwilligung freiwillig war und nicht auf der Erfüllung eines Vertrags basiert

Arten der Zustimmung:

- muss freigegeben werden
- Betroffener muss informiert werden, was Inhalt ist
- Klar: Verarbeiter darf keine Verarbeitungs-/Verwendungs-Zwecke verheimlichen
- Spezifisch: Zustimmung nur für bestimmten Grund gegeben

GDPR Art. 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

Wird einem Kind ein Angebot gemacht, das die Verarbeitung personenbezogener Daten enthält, muss ab dem 16. Lebensjahr das Kind zustimmen. Unter 16 müssen Eltern Erlaubnis geben

- Mitgliedsstaaten dürfen Grenzen bis 13. Lebensjahr legen

Erwägungsgrund 38 (Besonderer Schutz der Daten von Kindern)

Art 9. Spezielle Kategorien personenbezogener Daten

Personenbezogene Daten:

- Rasse oder ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Meinungen
- Gewerkschaftsangehörigkeiten
- Genetische oder Biometrische Daten
- Sex Life oder Orientierung

dürfen nicht verarbeitet werden, solange der Betroffene nicht ausdrücklich eingewilligt hat.

Ausnahmen wie gehabt (Ausübung Rechter und Pflichten, Schutz lebenswichtiger Interessen, Rechtsansprüche, ...)

Data Controller - Data Processor

- Processor muss die gleichen Grundsätze wie Controller verfolgen
- Processor muss alle Aktivitäten, die er für Controller vorgenommen hat, aufzeichnen
- Processor muss Vertrag oder legale Grundlage haben in dem beschrieben wird, was, wie lang, warum und welche Daten
- Processor muss Controller informieren, wenn andere "Sub" Processoren zugezogen werden

GDPR Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

Verantwortlicher trifft geeignete Maßnahmen um der betroffenen Person Inhalter aus Art. 13, 14, 15 in leichter Sprache zu vermitteln. Gilt besonders im Fall von Verarbeitung personenbezogener Daten von Kindern

GDPR Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

GDPR Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

GDPR Art. 15 Auskunftsrecht der betroffenen Person

GDPR Art. 16 Recht auf Berichtigung

GDPR Art. 17 Recht auf Löschung ("Recht auf Vergessenwerden")

1. Betroffene Person hat das Recht, dass personenbezogene Daten unverzüglich gelöscht werden sofern einer der folgenden Gründe zutrifft:
    - nicht mehr notwendig für urssprünglichen Zweck
    - Person widerruft gemäß Art. 6
    - Person legt Widerspruch ein
    - Daten wurden unrechtmäßig verarbeitet
    - Aufgrund rechtlicher Verpflichtung Löschung erforderlich
2. Wenn Verarbeiter Daten veröffentlicht hat, muss er diese Rückgängig machen und alle Maßnahmen ergreifen, damit dies geschieht
3. 1 und 2 gelten nicht, wenn einer oder mehrere der folgenden Gründe zutrifft:
    - Freie Meinungsäußerung
    - Erfüllung rechtlicher Pflichten
    - öffentliches Interesse
    - Archivzwecke, wissenschaftliche oder historische Forschungszweck

GDPR Art. 25 Datenschutz durch Technikgestaltung und durch Datenschutzfreundliche Voreinstellungen

1. Zur Sicherung der Daten muss geeignete technische Maßnahme ergriffen werden
2. Es muss technisch sichergestellt werden, dass nur erforderliche Daten gespeichert werden

3. Es kann zertifiziert werden, dass 1 und 2 eingehalten werden

GDPR Art. 30 Verzeichnis von Verarbeitungstätigkeiten

1. Verantwortlicher müssen Verzeichnis über alle Verarbeitungsaktivitäten führen
    1. Inhalt
    2. Zweck
    3. Was, Wie, Warum

GDPR Art. 32 Sicherheit der Verarbeitung

1. Angemessene Schutzmaßnahmen in Bezug auf Risiko

   a) Pseudonymisierung b) Systeme CIA sicherstellen c) Verfügbarkeit und Möglichkeit der Wiederherstellung sicherstellen d) Auditierung der Maßnahmen

2. Für Beurteilung des Schutzniveaus muss Risiko berücksichtigt werden besonders für Vernichtung, Verlust, Veränderung oder Offenlegung

3. Nur berechtigte dürfen Daten verarbeiten

GDPR Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

1. Meldung relevanter Vorfälle binnen 72 Stunden an Behörde
2. Verantwortlichen informieren
3. Alle den Vorfall betreffende relevante Informationen liefern

GDPR Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

1. Bei hohem Risiko muss betroffene Person unverzüglich informiert werden
2. Vorfall klar und verständlich beschreiben

GDPR Art. 35 Datenschutz-Folgenabschätzung

1. Wenn hohes Risiko vorliegt, muss vorher Abschätzung der Folgen/Auswirkungen vorgenommen werden
2. Einbeziehung Datenschutzbeauftragter
3. Besonders wichtig bei Art.9 (spezielle Kategorien), Strafvollzug
4. Liste durch Aufsichtsbehörde, die bei Folgeabschätzung abgearbeitet werden muss

Folgeabschätzung muss enthalten:

- systematische Beschreibung der geplanten Arbeitsvorgänge
- Bewerbung Notwendigkeit und Verhältnismäßigkeit
- Bewertung Risiken
- Abhilfemaßnahmen

GDPR Art. 36 Vorherige Konsultation

1. Bei Verarbeitung besonders kritischer Daten die nach Art. 35 Einschätzung zu hohes Risiko mit sich bringen muss Aufsichtsbehörde einbezogen werden
2. Wenn Aufsichtsbehörde nicht zustimmt, gibt Behörde Empfehlung
3. Verarbeiter muss alle Informationen offenlegen

GDPR Art. 37 Benennung eines Datenschutzbeauftragten

1. Datenschutzbeauftragter muss existieren, wenn:
    1. Behörde
    2. Umfangreiche, systematische Verarbeitung vorliegt
    3. Besondere Kategorien
2. Teilkonzerne können gemeinsamen Datenschutzbeauftragten haben
3. Bei Behörden nach Zweck gemeinsamer Datenschutzbeauftragter
4. Muss Qualifikationen vorweisen können
5. Intern oder extern
6. Wird Aufsichtsbehörde kommuniziert

GDPR Art. 38 Stellung des Datenschutzbeauftragten

1. Involvieren in alle relevanten Fälle
2. Verarbeiter muss Datenschutzbeauftragten unterstützen
3. Darf nicht benachteiligt werden
4. Muss Hilfestellung geben bei Bedarf
5. Muss geheim halten
6. Darf andere Tätigkeiten wahrnehmen, jedoch ohne Interessenskonflikt

4.2 International Data Protection Regulations

GDRP vs. Turkish Law 6698 (KVKK)

- Regularien ähnlich zu GDPR
- KVKK fordert nicht:
    - Datenschutzbeauftragten
    - Datenschutz-Folgeabschätzung
- KVKK fordert:
    - Alle Verarbeitungen müssen in VERBIS angegeben werden
- Strafen in KVKK niedriger

GDRP vs. LGPD (Brasilien)

- Regularien ähnlich zu GDPR
- Beide haben Datenschutzbeauftragten
- GDPR definiert Kriterien für Datenschutzbeauftragten
    - LGPD fordert in jedem Fall unabhängig von Kriterien
- LGPD hat Skala für Risiken
- LGPD gibt keine Fristen für das Melden von Vorfällen vor
- Strafen in LGPD geringer

GDRP vs. RUSSIAN FEDERATION FEDERAL LAW

- Keine Unterscheidung zwischen Controller und Processor
- Datenschutzbeauftragter darf nicht extern sein
- Registrierung aller Verarbeitungen von Roskomnadzor (Föderaler Dienst für die Aufsicht im Bereich der Kommunikation, Informationstechnologie und Massenkommunikation)
- Verarbeitung von persönlichen Daten darf nur in Russland erfolgen
- Keine Spezifizierung über Menge und Speicherungs-Dauer
- Keine Einschränkung durch Risiko, solange ausreichend geschützt
- Schutzmaßnahmen müssen zertifiziert sein
- Schwere Konsequenzen

GDPR vs. Thai Personal Data Protection Act (PDPA)

- Ähnlich zu GDPR
- Schriftliche Zustimmung notwendig, GDPR nur implizit
- Kinder ab 10
- Recht auf Löschung, nur wenn Verarbeiter nicht compliant ist, oder die Daten nicht mehr für den Zweck der Verarbeitung benötigt werden
- Widerruf: erhobene Daten dürfen weiterhin verarbeitet werden, jedoch keine neuen
- Niedrigere Strafen
- Datenschutzbeauftragter nur wenn:
    - Großer Umfang
    - Kernaktivität Verarbeitung sensibler Daten

GDPR vs. USA

- nur kleine Grundlagen von Datenschutz für US Bürger, für nicht US Bürger gar keine
- Schutz der Privatsphäre soll durch Gesetze geschützt werden
    - FISMA: IT Sec und Protection Programm für Behörden
    - HIPAA: Schutz von Gesundheitsdaten
    - NIST 800-171: Datenschutz unklassifizierter Informationen für nicht behördliche Verarbeitung
    - GLB: Schutz persönlicher Informationen in Finanzbehörden
- Handhabung unterschiedlich je nach Staat
    - California: Vorretier in USA. 2023 CPRA Erweiterung von CCPA -> Enforcement
    - Colorado
    - Virginia

GDPR vs. China Personal Information Protection Law (PIPL)

PIPL soll Rahmen schaffen, wie Unternehmen weltweit, in China als auch außerhalb, personenbezogene Daten verarbeiten, sammeln und weitergeben

Rechte für Personen

- Recht zu Wissen, was Unternehmen mit den Daten macht und machen wird
- Recht Entscheidung über Daten zu treffen
- Recht Verarbeitung einzuschränken oder zu verbieten

- Recht Daten einzusehen
- Recht auf Löschung
- Recht auf Übertragung
- Recht auf Auskunft über Regeln der Verarbeitung

Anforderungen PIPL

- Zustimmung von Person ➡️ GDPR
- Daten benötigt, um Vertrag zu erfüllen ➡️ GDPR
- Daten für HR benötigt, Arbeitsgesetze, Tarifverträge: ➡️ GDPR
- Daten für gesetzliche Aufgaben ➡️ GDPR
- Daten für öffentliches Interesse relevant ➡️ GDPR
- Person hat Daten bereits selber offengelegt ➡️ GDPR

Sensible Daten (GDPR spezielle Kategorien)

- Religion, Health, Finanzen, Biometrische Daten
- Risiko Analyse muss im Vorhinein durchgeführt werden

Besser in PIPL:

- Schulungen/Trainings für Umgang mit p. Daten für Mitarbeiter gefordert
- Datenweitergabe an Ausland ohne Zustimmung der Regierung untersagt
- Ohne Genehmigung dürfen nur Daten die nicht Artikel 9 sind nach China übertragen werden

GDPR vs. INAI (Mexico)

- Definition personenbezogener Daten gleich wie in GDPR
- Spezielle Kategorien sind in INAI Sensitive Personal Data
- Datenschutzbeauftragter gefordert

Grundsätze für Verarbeitung

- Transparent und fair ➡️ GDPR
- Eindeutig ➡️ GDPR
- Einwilligung muss eingeholt werden
- Verarbeitung nach Zweck der Erhebung ➡️ GDPR
- Korrekt und auf dem aktuellen Stand ➡️ GDPR
- Dauer nur dem Zweck ➡️ GDPR
- Betroffene können angemessen Privatsphäre erwarten
- Datenschutzhinweis kann gefordert werden

Einwilligung:

- Implizit
- Stillschweigend
- Ausdrücklich (Finanz und Vermögensdaten)

Keine Einwilligung erforderlich wenn:

- Durch Gesetz erforderlich ➡️ GDPR
- Daten von vornherein öffentlich zugänglich ➡️ GDPR
- Pseudonymisiert
- Pflichten Rechtsverhältnis ➡️ GDPR
- Notfallsituation ➡️ GDPR
- Medizinisch ➡️ GDPR
- Justiz ➡️ GDPR

Meldung Verletzungen

- bei Verlust, Zerstörung, Diebstahl, Nutzung Zugriff (unrechtmäßig)

Empfehlung an betroffene, was für Maßnahmen ergriffen werden sollten

Klarer als in GDPR geregelt: Benachrichtigung über Ursache, Hergang, Handlungsempfehlungen