Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 1. Übung vom 24.04.2023:

Einführung in den Datenschutz

1.1 Grundsätze

Aufgabe:

- Welche **Grundsätze** sind bei der Verarbeitung personenbezogener Daten nach der EU-DSGVO zu beachten? In welcher Höhe kann ein Bußgeld verhängt werden, wenn gegen diese Grundsätze verstoßen wird?

1.1 Grundsätze (1)

Art. 5 EU-DSGVO legt folgende Grundsätze für die Verarbeitung personenbezogener Daten fest:

1. **Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
   - Verarbeitung muss rechtmäßig sein (näher ausgeführt in Art. 6 EU-DSGVO)
   - Verarbeitung muss nach Treu und Glauben erfolgen (= gemäß gegenseitiger Erwartungshaltung)
   - Verarbeitung muss für die betroffene Person transparent sein (näher ausgeführt in Art. 12 – 15 EU-DSGVO)
2. **Grundsatz der Zweckbindung**
   - Zwecke müssen festgelegt, eindeutig und legitim sein
   - die Verarbeitung muss mit diesen Zwecken vereinbar sein
   - Privileg für Archivzwecke, für wissenschaftliche / historische Forschungs-zwecke und für statistische Zwecke

1.1 Grundsätze (2)

Art. 5 EU-DSGVO legt folgende Grundsätze für die Verarbeitung personenbezogener Daten fest:

3. Grundsatz der Datenminimierung

- Personenbezogene Daten müssen für den Zweck angemessen sein (=> Verhältnismäßigkeit für verfolgten Zweck)
- Personenbezogene Daten müssen für den Zweck erheblich sein (=> Eignung für verfolgten Zweck)
- Personenbezogene Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (=> Erforderlichkeit für verfolgten Zweck)

4. Grundsatz der Richtigkeit

- Personenbezogene Daten müssen sachlich richtig sein
- Personenbezogene Daten müssen auf aktuellem Stand sein
- Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden

1.1 Grundsätze (3)

Art. 5 EU-DSGVO legt folgende Grundsätze für die Verarbeitung personenbezogener Daten fest:

5. **Grundsatz der Speicherbegrenzung**
   - Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (näher ausgeführt in Art. 11 EU-DSGVO)
   - Längere Speicherung zulässig für Archivzwecke, für wissenschaftliche / historische Forschungszwecke und für statistische Zwecke, soweit geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen durchgeführt werden
6. **Grundsatz der Integrität und Vertraulichkeit**
   - Gewährleistung der angemessenen Sicherheit personenbezogener Daten
   - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
   - Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung

1.1 Grundsätze (4)

Art. 5 EU-DSGVO legt folgende Grundsätze für die Verarbeitung personenbezogener Daten fest:

7. **Grundsatz der Rechenschaftspflicht**
   - Der Verantwortliche ist für die Einhaltung der vorgenannten sechs Grundsätze verantwortlich
   - Der Verantwortliche muss dessen Einhaltung nachweisen können

Nach Art. 83 Abs. 5 lit. a EU-DSGVO können bei Verstöße gegen diese Grundsätze Geldbußen von bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden

1.2 Schutzziele

Aufgabe:

- Welche **Schutzziele** müssen Systeme oder Dienste, mit denen personenbezogene Daten verarbeitet werden, berücksichtigen? Ordnen Sie die Angaben aus Art. 32 Abs. 1 lit. c EU-DSGVO und Art. 32 Abs. 2 EU-DSGVO diesen Schutzzielen zu!

1.2 Schutzziele

Schutzziel	Ausprägung
Vertraulichkeit	Keine unbefugte **Offenlegung** von personenbezogenen Daten
	Kein unbefugter **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden
Integrität	Keine unbeabsichtigte oder unrechtmäßige **Veränderung** von personenbezogenen Daten
	Keine unbeabsichtigte oder unrechtmäßige **Vernichtung** von personenbezogenen Daten
	Kein unbeabsichtigter oder unrechtmäßiger **Verlust** von personenbezogenen Daten
Verfügbarkeit	Keine unbeabsichtigte oder unrechtmäßige **Vernichtung** von personenbezogenen Daten
	Kein unbeabsichtigter oder unrechtmäßiger **Verlust** von personenbezogenen Daten
	Rasche **Wiederherstellung** der Verfügbarkeit von bzw. dem Zugang auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall
Belastbarkeit	Rasche **Wiederherstellung** der Verfügbarkeit von bzw. dem Zugang auf personenbezogene Daten bei einem physischen oder technischen Zwischenfall

1.3 Betroffenenrechte

Aufgabe:

- Welche **Rechte** haben **betroffene Personen** nach der EU-DSGVO?

1.3 Betroffenenrechte (1)

Die betroffene Person hat folgende Rechte:

- **Recht auf transparente Information** nach Art. 12 EU-DSGVO
  - in präziser, transparenter, verständlicher und leicht zugänglicher Form
  - in einer klaren und einfachen Sprache
  - unentgeltlich, soweit nicht offenkundig unbegründet oder exzessiv genutzt
  - Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Art. 15 – 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber i.d.R. innerhalb eines Monats nach Eingang des Antrags zur Verfügung oder unterrichtet die betroffene Person über eine aufgrund der Komplexität bzw. der Anzahl von Anträgen benötigten Fristverlängerung => Bei Verzögerung ist die betroffene Person auf die Möglichkeit hinzuweisen, Beschwerde bei der Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einlegen zu können

1.3 Betroffenenrechte (2)

Die betroffene Person hat folgende Rechte:

- **Recht auf Information** bei der Erhebung personenbezogener Daten nach Art. 13 EU-DSGVO
  - Namen und Kontaktdaten des Verantwortlichen
  - Kontaktdaten des Datenschutzbeauftragten
  - Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
  - die Rechtsgrundlage für die Verarbeitung
  - berechtigte Interessen, die von dem Verantwortlichen oder einem Dritten nach Art. 6 Abs. 1 lit. f EU-DSGVO verfolgt werden
  - gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
  - gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und die hierfür bestehende Garantie
  - die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

1.3 Betroffenenrechte (3)

Die betroffene Person hat folgende Rechte:

- **Recht auf Information** bei der Erhebung personenbezogener Daten nach Art. 13 EU-DSGVO (1. Fortsetzung)
  - das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit
  - das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, soweit die Verarbeitung auf Art. 6 Abs. 1 lit. a EU-DSGVO oder Art. 9 Abs. 2 lit. a EU-DSGVO beruht
  - das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  - ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte

1.3 Betroffenenrechte (4)

Die betroffene Person hat folgende Rechte:

- **Recht auf Information** bei der Erhebung personenbezogener Daten nach Art. 13 EU-DSGVO (2. Fortsetzung)
  - das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 EU-DSGVO und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
  - Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung

1.3 Betroffenenrechte (5)

Die betroffene Person hat folgende Rechte:

- **Recht auf Information** zur Erhebung personenbezogener Daten, die nicht beim Betroffenen erfolgt, nach Art. 14 EU-DSGVO
  - Analog zu Art. 13 EU-DSGVO, aber ohne die Information darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
  - Zusätzlich die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden, wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f EU-DSGVO beruht
  - Zusätzlich aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen
  - Die Informationen sind spätestens innerhalb eines Monats bzw. zum Zeitpunkt der Offenlegung an einen anderen Empfänger zu erteilen
  - Die Information kann unterbleiben, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt, sich die die Erteilung dieser Informationen als unmöglich erweist bzw. einen unverhältnismäßigen Auf-wand erfordern würde oder die Erlangung bzw. Offenlegung gesetzlich ausdrücklich vorgeschrieben ist oder auf einem Berufsgeheimnis basiert

1.3 Betroffenenrechte (6)

Die betroffene Person hat folgende Rechte:

- **Recht auf Auskunft** nach Art. 15 EU-DSGVO
  - Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, und falls dies der Fall ist:
  - die Verarbeitungszwecke
  - die Kategorien personenbezogener Daten, die verarbeitet werden
  - die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen
  - falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
  - das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung

1.3 Betroffenenrechte (7)

Die betroffene Person hat folgende Rechte:

- **Recht auf Auskunft** nach Art. 15 EU-DSGVO (Fortsetzung)
  - das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  - wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
  - das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 EU-DSGVO und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
  - Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Art. 46 EU-DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden
  - Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung

1.3 Betroffenenrechte (8)

Die betroffene Person hat folgende Rechte:

- **Recht auf Berichtigung** nach Art. 16 EU-DSGVO
  - Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen
  - Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen
- **Recht auf Löschung** („Recht auf Vergessenwerden“) nach Art. 17 EU-DSGVO
  - Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern
  - die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind

1.3 Betroffenenrechte (9)

Die betroffene Person hat folgende Rechte:

- **Recht auf Löschung** („Recht auf Vergessenwerden“) nach Art. 17 EU-DSGVO (1. Fortsetzung)
  - Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern
  - die betroffene Person ihre Einwilligung widerruft hat
  - die betroffene Person gemäß Art. 21 Abs. 1 EU-DSGVO Widerspruch gegen die Verarbeitung eingelegt hat
  - die personenbezogenen Daten unrechtmäßig verarbeitet wurden
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, dem der Verantwortliche unterliegt
  - die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft für Kinder gemäß Art. 8 Abs. 1 EU-DSGVO erhoben wurden

1.3 Betroffenenrechte (10)

Die betroffene Person hat folgende Rechte:

- **Recht auf Löschung** („Recht auf Vergessenwerden“) nach Art. 17 EU-DSGVO (2. Fortsetzung)
  - Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat
  - Eine Löschung ist <u>nicht</u> erforderlich, wenn die Verarbeitung erfolgt
    - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
    - zur Erfüllung einer rechtlichen Verpflichtung
    - aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h und i EU-DSGVO sowie Art. 9 Abs. 3 EU-DSGVO
    - für Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke
    - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

1.3 Betroffenenrechte (11)

Die betroffene Person hat folgende Rechte:

- **Recht auf Einschränkung** der Verarbeitung nach Art. 18 EU-DSGVO
  - Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn
    - die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird für die Dauer der Überprüfung
    - die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt
    - der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt
    - die betroffene Person Widerspruch gegen die Verarbeitung gemäß Art. 21 Abs. 1 EU-DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen
  - Eine betroffene Person, die eine Einschränkung der Verarbeitung erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird

1.3 Betroffenenrechte (12)

Die betroffene Person hat folgende Rechte:

- **Recht auf Mitteilung** über Berichtigung, Löschung oder Einschränkungen nach Art. 19 EU-DSGVO
  - Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden
  - Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt
- **Recht auf Datenübertragbarkeit** nach Art. 20 EU-DSGVO
  - Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten
  - Die betroffene Person hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln

1.3 Betroffenenrechte (13)

Die betroffene Person hat folgende Rechte:

- **Recht auf Datenübertragbarkeit** nach Art. 20 EU-DSGVO (Forts)
  - Die betroffene Person hat das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist
  - Das Recht auf Datenübertragbarkeit darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen
- **Recht auf Widerspruch** nach Art. 21 EU-DSGVO
  - Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffen-der personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f EU-DSGVO erfolgt sowie bei Profiling, Widerspruch einzulegen
  - Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Aus-übung oder Verteidigung von Rechtsansprüchen

1.3 Betroffenenrechte (14)

Die betroffene Person hat folgende Rechte:

- **Recht auf Widerspruch** nach Art. 21 EU-DSGVO (Fortsetzung)
  - Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für Profiling, soweit dies mit solcher Direktwerbung in Verbindung steht
  - Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet
  - Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf ihr Widerspruchsrecht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen
  - Auch in den privilegierten Fällen darf infolge der besonderen Situation der betroffenen Person ein Widerspruch eingelegt werden, soweit die Verarbeitung nicht zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist

1.3 Betroffenenrechte (15)

Die betroffene Person hat folgende Rechte:

- **Recht auf Nichtausschließlichkeit automatisierter Entscheidung** nach Art. 22 EU-DSGVO
  - Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, sofern die Entscheidung nicht
    - für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist
    - aufgrund von Rechtsvorschriften, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten
    - mit ausdrücklicher Einwilligung der betroffenen Person erfolgt
  - Bei Vertrag oder Einwilligung trifft der Verantwortliche angemessene Maß-nahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren (=> Prüfung durch natürliche Person)

1.4 Datenschutzverletzung

Aufgabe:

- Was ist im Falle einer **Verletzung des Schutzes von personenbezogenen Daten** zu tun? Begründen Sie Ihre Antwort! (d.h. belegen Sie Ihre Antwort unter Angabe entsprechender Rechtsquellen)

1.4 Datenschutzverletzung (1)

- Unter einer Verletzung des Schutzes personenbezogener Daten ist nach Art. 4 Nr. 12 EU-DSGVO zu verstehen eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig
  - zur **Vernichtung** von personenbezogenen Daten,
  - zum **Verlust** von personenbezogenen Daten,
  - zur **Veränderung** von personenbezogenen Daten,
  - zur **unbefugten Offenlegung** von personenbezogenen Daten oder
  - zum **unbefugten Zugang** zu personenbezogenen Daten

  führt, die übermittelt, gespeichert oder sonstige Weise verarbeitet wurden
  → Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO verletzt
  → betrifft sowohl eine absichtliche Verletzung (→ Angriff von Intern oder Extern) als auch eine versehentliche Verletzung (→ Fahrlässigkeit)
- Solche Fälle sind binnen 72 Stunden der Aufsichtsbehörde nach Art. 33 EU-DSGVO zu melden und darüber u.U. unverzüglich die betroffene Person nach Art. 34 EU-DSGVO zu benachrichtigen

1.4 Datenschutzverletzung (2)

- Die Meldung nach Art. 33 Abs. 1 EU-DSGVO muss erfolgen, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen
  → Verantwortlicher muss Verletzung erst mal feststellen
  → Verantwortlicher muss entsprechende Detektions- und Meldeprozesse etablieren
  → Nach Feststellung ist zunächst zu prüfen, ob aus der Verletzung ein Risiko für die Rechte und Freiheiten mind. 1 natürlicher Person resultieren kann
  → Nach ErwG 85 EU-DSGVO geht nur dann kein Risiko von einer Datenschutzverletzung aus, wenn der Verantwortliche dies selbst nach Art. 5 Abs. 2 EU-DSGVO nachweisen kann
- Auftragsverarbeiter haben den Verantwortlichen eine Datenschutzverletzung unverzüglich zu melden nach Art. 33 Abs. 2 EU-DSGVO
- Meldungen an die Aufsichtsbehörde haben nach Art. 33 Abs. 3 EU-DSGVO folgende Informationen zu enthalten:
  - Beschreibung der Art der Datenschutzverletzung, möglichst mit Angabe der Kategorie und ungefähren Zahl betroffener Personen als auch mit Angabe der Kategorie und ungefähren Zahl betroffener Datensätze

1.4 Datenschutzverletzung (3)

- Meldungen an die Aufsichtsbehörde haben nach Art. 33 Abs. 3 EU-DSGVO folgende Informationen zu enthalten: (Fortsetzung)
  - Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
  - Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung
  - Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und ggf. von Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkung

  → Datenschutzverletzung ist näher zu analysieren (Betroffene & Datenarten)
  → Analyse der wahrscheinlichen Folgen
  → Gewichtung potenzieller Folgen hinsichtlich Eintrittswahrscheinlichkeit
  → Prüfung, welche Maßnahmen zur Behebung der Datenschutzverletzung zu ergreifen sind
  → Verhinderung einer Wiederholungsgefahr
  → Abmilderung negativer Folgen für Betroffene
- Datenschutzverletzungen sind zu dokumentieren nach Art. 33 Abs. 5 EU-DSGVO

1.4 Datenschutzverletzung (4)

- Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, hat der Verantwortliche nach Art. 34 Abs. 1 EU-DSGVO die betroffene Person unverzüglich und nach Art. 34 Abs. 2 EU-DSGVO in klarer und einfacher Sprache mit den gleichen Informationen zu benachrichtigen
  → Bewertung des Risikos für die persönlichen Rechte und Freiheiten der Betroffenen zu ermitteln
  → Berücksichtigung der individuellen Risiken (→ keine globale Betrachtung)
- Eine Benachrichtigung der betroffenen Personen ist nicht erforderlich, wenn
  - der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen vor der Datenschutzverletzung getroffen hat, die einen unbefugten Zugang zu den Daten verhindern sollen (→ präventiver Schutz)
  - der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht (→ reaktiver Schutz)
  - die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre (→ dann: öffentliche Bekanntmachung nötig)

1.5 Privacy by Design & Default

Aufgabe:

- Geben Sie mind. 3 frei gewählte Beispiele, wie nach Art. 25 EU-DSGVO
  a) **Datenschutz durch Technikgestaltung**
  b) **Datenschutz durch datenschutzfreundliche Voreinstellungen** jeweils erreicht werden kann!

1.5 Privacy by Design & Default (1)

a) 3 Beispiele für **Datenschutz durch Technikgestaltung**:

- Die Verarbeitung berücksichtigt eine frühzeitige Pseudonymisierung personenbezogener Daten mit entsprechender Separierung des Zuordnungsmerkmals, ohne dass dies im Verarbeitungssystem selbst wieder zusammengeführt werden kann
- Das Verarbeitungssystem verfügt über Funktionen, die der Betroffene selbst oder über einen Vertreter nutzen kann, um sich die zu seiner Person gespeicherten Daten einsehen zu können
- Die vom Verarbeitungssystem verarbeiteten Daten werden verschlüsselt gespeichert

1.5 Privacy by Design & Default (2)

b) 3 Beispiele für **Datenschutz durch datenschutzfreundliche Voreinstellung**:

- Das Verarbeitungssystem weist Funktionen auf zur Übertragbarkeit (Exportierbarkeit an vom Betroffenen benannten Stellen) von Daten und fristgerechten Löschung der Daten
- Der durch das Verarbeitungssystem verwendete Datenumfang ist auf das absolut Notwendige beschränkt, das zur Zweckerfüllung benötigt wird
- Das Verarbeitungssystem verfügt über ein umfassendes Berechtigungskonzept, mit dem ein differenziertes Berechtigungswesen abgebildet werden kann, das den generellen Zugriff nach dem Need-to-know-Prinzip gewährt und den Zugriff auf besonders schützenswerte Daten nur unter Einhaltung eines 4-Augen-Prinzips zulässt