Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 2. Übung im SoSe 2019:

Einführung in den Datenschutz
nach der EU-DSGVO (2)

2.1 Gesundheitsdatenverarbeitung

Aufgabe:

- Welche besonderen Rechtsvorschriften zur Verarbeitung von **Gesundheitsdaten** weist die EU-DSGVO auf?

2.1 Gesundheitsdatenverarbeitung (1)

- **Gesundheitsdaten** sind nach Art. 4 Nr. 15 EU-DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen
- Gesundheitsdaten zählen zu den besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 EU-DSGVO
- Ein Verbot zur Verarbeitung von Gesundheitsdaten besteht nach Art. 9 Abs. 2 EU-DSGVO nicht, wenn
  a) die betroffene Person ausdrücklich eingewilligt hat [im Kundendatenschutz der Regelfall, soweit es sich nicht um medizinische Versorgung handelt]
  b) die Verarbeitung nach Arbeitsrecht bzw. dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist [z.B. AU-Bescheinigung, BEM]
  c) die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben

2.1 Gesundheitsdatenverarbeitung (2)

- Ein Verbot zur Verarbeitung von Gesundheitsdaten besteht nach Art. 9 Abs. 2 EU-DSGVO nicht, wenn
  - d) die Verarbeitung auf der Grundlage geeigneter Garantien eines sog. Tendenzbetriebs erfolgt und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden
  - e) die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat [muss beweisbar sein!]
  - f) die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist
  - g) die Verarbeitung aufgrund spezifischen Rechts erforderlich ist und dabei der Wesensgehalt des Datenschutzrechts gewahrt wird und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorgesehen sind

2.1 Gesundheitsdatenverarbeitung (3)

- Ein Verbot zur Verarbeitung von Gesundheitsdaten besteht nach Art. 9 Abs. 2 EU-DSGVO nicht, wenn
  - h) die Verarbeitung erforderlich ist
    - zur Gesundheitsvorsorge oder der Arbeitsmedizin, [Unfallbehandlung]
    - für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, [Einstellung]
    - für die medizinische Diagnostik,
    - für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich
    - oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich nach geltendem Recht
  - i) die Verarbeitung im Bereich der öffentlichen Gesundheit nach geltendem Recht unter Wahrung des Berufsgeheimnisses erforderlich ist, wie
    - dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder
    - zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung, bei Arzneimitteln sowie Medizinprodukten

2.1 Gesundheitsdatenverarbeitung (4)

- Ein Verbot zur Verarbeitung von Gesundheitsdaten besteht nach Art. 9 Abs. 2 EU-DSGVO nicht, wenn
  j) die Verarbeitung nach geltendem Recht erforderlich ist für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke
- Die Verarbeitung nach Art. 9 Abs. 2 lit. h EU-DSGVO setzt nach Art. 9 Abs. 3 EU-DSGVO voraus, dass diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt (= ärztliche Schweigepflicht bzw. Betriebsanitäter)
- Bei einer Zweckänderung von Gesundheitsdaten ist dem Umstand, dass es sich um Gesundheitsdaten handelt, besonders Rechnung zu tragen (Art. 6 Abs. 4 lit. c EU-DSGVO)
- Basiert die Verarbeitung auf der Einwilligung der betroffenen Person nach Art. 9 Abs. 2 lit. a EU-DSGVO, muss der Verantwortliche zum Zeitpunkt der Erhebung der Gesundheitsdaten auf das Widerrufsrecht nach Art. 13 Abs. 2 lit. c EU-DSGVO bzw. innerhalb eines Monats nach Art. 14 Abs. 2 lit. d EU-DSGVO bei Erhebung an anderer Stelle hinweisen

2.1 Gesundheitsdatenverarbeitung (5)

- Ein Recht auf Löschung besteht nach Art. 17 Abs. 3 lit. c EU-DSGVO nicht, wenn die Verarbeitung von Gesundheitsdaten erforderlich ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit nach Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 EU-DSGVO
- Basiert die Verarbeitung auf der Grundlage einer Einwilligung nach Art. 9 Abs. 1 lit. a EU-DSGVO, hat die betroffene Person das Recht auf Datenübertragbarkeit nach Art. 20 Abs. 1 lit. a EU-DSGVO
- Automatisierte Entscheidungen nach Art. 22 Abs. 2 EU-DSGVO, insbesondere für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen sowie mit ausdrücklicher Einwilligung der betroffenen Person, dürfen nach Art. 22 Abs. 4 EU-DSGVO nicht auf Gesundheitsdaten beruhen, sofern die Verarbeitung nicht auf Art. 9 Abs. 2 lit. a (Einwilligung) oder g (Bereichsrecht) beruht und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden
- Bei einer umfangreichen Verarbeitung von Gesundheitsdaten ist nach Art. 35 Abs. 3 lit. b EU-DSGVO eine Datenschutz-Folgenabschätzung durchzuführen

2.1 Gesundheitsdatenverarbeitung (6)

- Wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung von Gesundheitsdaten besteht, ist nach Art. 37 Abs. 1 lit. c EU-DSGVO ein Datenschutzbeauftragter zu benennen
- Verstöße gegen Art. 9 EU-DSGVO können nach Art. 83 Abs. 5 lit. a EU-DSGVO zu einem Bußgeld in Höhe von 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres führen

2.2 Verzeichnis von Verarbeitungstätigkeiten

Aufgabe:

- Erstellen Sie gemäß den Anforderungen aus Art. 30 EU-DSGVO für einen Verantwortlichen das **Verzeichnis von Verarbeitungstätigkeiten** zu einem selbst gewählten Verfahren des **Kundendatenschutzes**, welches mit einem IT-System durchgeführt wird!

2.2 Verzeichnis von Verarbeitungstätigkeiten (1)

1. **Name und Kontaktdaten des Verantwortlichen**:
   XY GmbH
   Musterstr. 1
   12345 Musterstadt
   Tel: 01234/56789-0, Mail: info@xy-gmbh.de
   Datenschutzbeauftragter: Manfred Mustermann
   Tel: 01234/56789-9, Mail: datenschutz@xy-gmbh.de
2. **Zwecke der Verarbeitung**:
   Newsletterabwicklung
3. **Kategorien betroffener Personen und Kategorien personenbezogener Daten**:
   Betroffene Personen: Kunden oder Interessenten
   Datenkategorien: Identifikationsdaten, Maildaten, Daten über Bezug & Abbestellung des Newsletters

2.2 Verzeichnis von Verarbeitungstätigkeiten (2)

4. **Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. noch offengelegt werden**:
   entfällt
5. **Datenübermittlung in Drittstaaten**:
   entfällt
6. **Vorgesehene Fristen für die Löschung der Daten**:
   6 Jahre (Geschäftsbriefe)
   1,5 Jahre für Einwilligungen ohne Newsletterversand
7. **Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen**:
   siehe spezifisches Sicherheitskonzept

2.3 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!

2.3 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

2.4 Datenschutzverletzung

Aufgabe:

- Was ist im Falle einer **Verletzung des Schutzes von personenbezogenen Daten** zu tun? Begründen Sie Ihre Antwort!

2.4 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

2.4 Datenschutzverletzung (2)

- Nach Art. 33 Abs. 1 EU-DSGVO hat der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, die Datenschutzverletzung zu melden, 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 natürlicher Personen (Plural!) resultieren 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

2.4 Datenschutzverletzung (3)

- Meldungen an die Aufsichtsbehörde haben nach Art. 33 Abs. 3 EU-DSGVO folgende Informationen zu enthalten:
  - 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

2.4 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)

2.5 CRM-System

Aufgabe:

- Ein Unternehmen möchte ein datenschutzkonformes **Customer-Relationship-Management-System** (CRM-System) einführen. In diesem CRM-System sollen alle kundenspezifische Daten zusammengetragen werden, die das Unternehmen bereits in verschiedenen Quellen gespeichert hat. Zu den Kunden zählen ausschließlich Privatpersonen. Wie muss das Unternehmen hierzu vorgehen? Begründen Sie Ihre Antwort!

2.5 CRM-System (1)

- Unternehmen = nicht-öffentliche Stelle
- CRM-System = System zur Kunden**bewertung** von wirtschaftlicher Lage, persönlicher Vorlieben, (Kauf-) Interessen, (Zahlungs-) Zuverlässigkeit & (Bestell- und Reklamations-) Verhalten
  → Profiling nach Art. 4 Nr. 4 EU-DSGVO
  → Datenschutz-Folgenabschätzung nötig nach Art. 35 Abs. 3 lit. a EU-DSGVO
  → Verhinderung einer Verarbeitung mit hohem Risiko für die Rechte und Freiheiten der Betroffenen
  → umfassende Schutzmaßnahmen nach Art. 32 EU-DSGVO erforderlich!

2.5 CRM-System (2)

- Nach Art. 35 Abs. 7 EU-DSGVO ist in der Datenschutz-Folgenabschätzung zumindest Folgendes zu behandeln:
  - Beschreibung der geplanten Verarbeitungsvorgänge
    → Detaillierte Festlegung der Verarbeitungsschritte
  - Verfolgte Zwecke und berechtigte Interessen
    → für jeden Schritt muss ein legitim verfolgter Zweck bestehen
    → bei berechtigten Interessen Abwägung darstellen, um Widerspruchsrechte der Betroffenen nach Art. 21 Abs. 1 EU-DSGVO abwehren zu können
  - Bewertung zur Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf die verfolgten Zwecke
  - Zur Bewältigung der Risiken geplante technische und organisatorische Abhilfemaßnahmen darstellen

2.5 CRM-System (3)

- Die Grundsätze aus Art. 5 Abs. 1 EU-DSGVO müssen für das CRM-System eingehalten werden
  → u.a. Datenminimierung & Speicherbegrenzung beachten
  → Import aus anderen Datenquellen muss mit den dafür ursprünglich festgelegten Zwecken vereinbar sein, sonst wird eine Informationspflicht ausgelöst nach Art. 14 Abs. 4 EU-DSGVO
  → sinnvollerweise dies bereits bei Datenschutz-Folgenabschätzung berücksichtigen
- Sofern ein DSB benannt wurde, diesen bei der Datenschutz-Folgenabschätzung anhören
- CRM-System ist in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO aufzunehmen