IHK Datenschutzbeauftragter Prüfung 2024 Praktisch – Lösungen

Teil A – Rechtsgrundlagen und Grundbegriffe (20 Punkte)

A1) Begriffsdefinitionen und Rechtsgrundlagen:
a) Verantwortlicher: Eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Rechtsgrundlage: Art. 4 Abs. 7 GDPR.
b) Auftragsverarbeiter: Eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Rechtsgrundlage: Art. 4 Abs. 8 GDPR.
c) Betroffene Person: Eine identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden. Rechtsgrundlage: Art. 4 Abs. 1 GDPR.
d) Personenbezogenes Datum: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Rechtsgrundlage: Art. 4 Abs. 1 GDPR.

A2) Rechtsgrundlage für Videoüberwachung: Die Videoüberwachung auf öffentlichem Gelände kann auf Art. 6 Abs. 1 lit. f GDPR gestützt werden, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Eine Interessenabwägung ist notwendig, um sicherzustellen, dass die Überwachung verhältnismäßig ist und keine übermäßige Beeinträchtigung der Privatsphäre der betroffenen Personen darstellt.

A3) Bußgeldtatbestände:
1. Verletzung der Grundsätze der Verarbeitung (Art. 5 GDPR) – Höchstsumme: 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes.
2. Nichteinhaltung der Rechte der betroffenen Person (Art. 12-22 GDPR) – Höchstsumme: 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes.
3. Nichteinhaltung der Pflichten des Verantwortlichen und des Auftragsverarbeiters (Art. 25-39 GDPR) – Höchstsumme: 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes.

Teil B – Technische und Organisatorische Maßnahmen (TOM) (20 Punkte)

B1) Verschlüsselung in Ruhe vs. Verschlüsselung in Übertragung:
- Verschlüsselung in Ruhe: Daten werden verschlüsselt, während sie gespeichert sind. Beispiel: Verschlüsselung einer Datenbank auf einem Server.
- Verschlüsselung in Übertragung: Daten werden verschlüsselt, während sie über ein Netzwerk übertragen werden. Beispiel: SSL/TLS-Verschlüsselung bei der Übertragung von Daten über das Internet.

B2) Speicherbedarf der Backup-Strategien:
- Vollbackup täglich: 30 Tage x 50 GB = 1500 GB.
- Differenzielles Backup: 1 Vollbackup (50 GB) + 29 Tage x 10 GB = 340 GB.
- Inkrementelles Backup: 1 Vollbackup (50 GB) + 29 Tage x 5 GB = 195 GB.
Empfehlung: Inkrementelles Backup, da es den geringsten Speicherbedarf hat und dennoch regelmäßige Sicherungen bietet.

B3) Organisatorische Maßnahmen:
- Zutrittskontrolle: Sicherheitsdienst, Zugangskarten.
- Zugriffskontrolle: Passwortschutz, Benutzerrollen.
- Weitergabekontrolle: Verschlüsselung, Protokollierung.

Teil C – Datenschutz-Folgenabschätzung (DSFA) (20 Punkte)

C1) Kernelemente einer DSFA:
- Risiko: Unbefugter Zugriff auf Gesundheitsdaten.
- Schwere der Auswirkung: Hoch.
- Maßnahme: Implementierung von Zwei-Faktor-Authentifizierung.

C2) Prüfauftrag: Der Datenschutzbeauftragte soll die Einhaltung der Datenschutzvorgaben bei der Einführung der Video-Telemedizin prüfen. Ziel ist es, Risiken zu identifizieren und geeignete Maßnahmen zur Risikominderung zu empfehlen. Der Umfang umfasst die Analyse der Datenverarbeitung und die Überprüfung der technischen und organisatorischen Maßnahmen.

C3) Risikoergebnis: Bei einem hohen Risiko ist die Aufsichtsbehörde einzubeziehen. Artikel: Art. 36 GDPR.

Teil D – Auftragsverarbeitung und Verträge (20 Punkte)

D1) Fehlender Artikel: Art. 28 Abs. 2 GDPR. Vertragsbaustein: „Der Auftragsverarbeiter darf keine weiteren Auftragsverarbeiter ohne vorherige spezifische oder allgemeine schriftliche Genehmigung des Verantwortlichen beauftragen."

D2) Pflichtinhalte eines AV-Vertrages:
1. Löschung nach Vertragsende – Art. 28 Abs. 3 lit. g GDPR.
2. Schutz technischer Anlagen – Art. 32 GDPR.
3. Information über Datenpannen – Art. 33 GDPR.
4. Vertraulichkeit – Art. 28 Abs. 3 lit. b GDPR.

D3) Unterschied:
- Joint Controller Agreement: Gemeinsame Verantwortlichkeit für die Verarbeitung, gemeinsame Festlegung der Zwecke und Mittel.
- AV-Vertrag: Auftragsverarbeiter handelt im Auftrag des Verantwortlichen, keine eigene Entscheidungsbefugnis.

Teil E – Praxisfall: Datenschutzkonzept (20 Punkte)

E1) Datenschutzkonzept:
a) Datenflussübersicht: Skizze der Erhebung, Verarbeitung und Speicherung von Gesundheits- und Ernährungsdaten.
b) Rechtsgrundlagen: Einwilligung der betroffenen Personen, Art. 6 Abs. 1 lit. a GDPR.
c) Betroffenenrechte: Verfahren zur Auskunft, Berichtigung, Löschung und Widerspruch.
d) Interne Schulungsmaßnahmen: Regelmäßige Schulungen zu Datenschutz und Datensicherheit für Mitarbeiter.