IHK Datenschutzbeauftragter Prüfung 2022 Praktisch – Lösungen

Teil 1: Rechtsgrundlagen und zentrale Begriffe (20 Punkte)

1. Definitionen (je 2 Punkte)
a) Personenbezogene Daten: Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören z.B. Name, Adresse, Geburtsdatum.
b) Verarbeitung: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang im Zusammenhang mit personenbezogenen Daten, wie das Erheben, Erfassen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
c) Einwilligung: Freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

2. Rechtsquellen in der korrekten Rangfolge (5 Punkte)
1. EU-Grundrechtecharta
2. Datenschutz-Grundverordnung (DSGVO)
3. BDSG-neu
4. Landesdatenschutzgesetze

3. Verantwortlicher vs. Auftragsverarbeiter (3 Punkte)
Verantwortlicher: Bestimmt allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten. Auftragsverarbeiter: Verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen und hat keine Entscheidungsbefugnis über die Zwecke und Mittel der Verarbeitung.

4. Zweckbindung und Speicherbegrenzung im Personalwesen (6 Punkte)
Zweckbindung: Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Beispiel: Erhebung von Mitarbeiterdaten zur Gehaltsabrechnung. Speicherbegrenzung: Daten müssen gelöscht werden, wenn sie für den Zweck nicht mehr erforderlich sind. Beispiel: Löschen von Bewerberdaten nach Abschluss des Bewerbungsverfahrens, sofern keine Einwilligung zur weiteren Speicherung vorliegt.

Teil 2: Fallstudie Online-Shop „TechTrend" (30 Punkte)

a) Datenerhebung von Geburtsdatum und E-Mail-Adresse (8 Punkte)
Mögliche Rechtsgrundlagen: Art. 6 Abs. 1 lit. a (Einwilligung) und lit. f (berechtigtes Interesse) DSGVO. Begründung: Für den Newsletter ist eine Einwilligung erforderlich, da es sich um Direktmarketing handelt. Das Geburtsdatum könnte für personalisierte Angebote relevant sein, jedoch muss die Notwendigkeit und Verhältnismäßigkeit geprüft werden.

b) Löschkonzept (4 Punkte)
Bestelldaten: 10 Jahre (steuerrechtliche Aufbewahrungspflicht)
Newsletter-Abonnenten: Bis zur Abmeldung oder Widerruf der Einwilligung
Supportanfragen: 2 Jahre nach Abschluss der Anfrage

c) Risikoanalyse für Datenpanne (6 Punkte)
Risiken:
- Unbefugter Zugriff auf Kundendaten (hoch, Schaden: hoch)
- Datenverlust durch Systemfehler (mittel, Schaden: mittel)
- Phishing-Angriffe auf Mitarbeiter (hoch, Schaden: hoch)

d) Bußgeldhöhe nach Art. 83 DSGVO (6 Punkte)
Berechnung: 5 Mio. € x 10% = 500.000 € (maximale Bußgeldhöhe bei schwerwiegender Fahrlässigkeit)

e) Pflichten zur Meldung der Panne (6 Punkte)
- Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden
- Information der betroffenen Personen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht
- Dokumentation der Panne und der ergriffenen Maßnahmen

Teil 3: Technische und organisatorische Maßnahmen (20 Punkte)

a) Netzwerkarchitektur (6 Punkte)
Skizze: DMZ zwischen Internet und Intranet, VPN-Zugang für externe Mitarbeiter, Schutzebenen durch Firewalls und IDS/IPS.

b) 4-Augen-Prinzip im Dokumentenmanagementsystem (4 Punkte)
- Implementierung von Freigabeworkflows, die eine zweite Person zur Bestätigung erfordern
- Protokollierung aller Freigabeprozesse

c) Funktionsweise von TLS und AES (5 Punkte)
TLS: Verschlüsselt Datenübertragungen im Internet, sichert die Verbindung zwischen Client und Server.
AES: Symmetrisches Verschlüsselungsverfahren, das Daten in Blöcken verschlüsselt und entschlüsselt.

d) Konzept für Mitarbeiterschulung (5 Punkte)
Zielgruppen: Alle Mitarbeiter, besonders IT und HR
Inhalte: Datenschutzgrundlagen, Umgang mit personenbezogenen Daten, Meldepflichten
Häufigkeit: Jährlich, mit Auffrischung bei Gesetzesänderungen

Teil 4: Datenschutz-Folgenabschätzung (DSFA) (20 Punkte)

a) Ablauf einer DSFA (8 Punkte)
1. Beschreibung der geplanten Verarbeitungsvorgänge
2. Bewertung der Notwendigkeit und Verhältnismäßigkeit
3. Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
4. Festlegung von Maßnahmen zur Risikominderung
5. Konsultation der Aufsichtsbehörde bei hohem Risiko
6. Dokumentation der DSFA-Ergebnisse

b) Risikomatrix (8 Punkte)
Risiken:
- Unbefugter Zugriff: Eintrittswahrscheinlichkeit hoch, Schadensschwere hoch
- Systemausfall: Eintrittswahrscheinlichkeit mittel, Schadensschwere mittel
- Datenweitergabe: Eintrittswahrscheinlichkeit niedrig, Schadensschwere hoch

c) Maßnahmen und Wirksamkeit (4 Punkte)
- Zugangskontrollen: Hoch wirksam gegen unbefugten Zugriff
- Redundante Systeme: Mittel wirksam gegen Systemausfall
- Verschlüsselung: Hoch wirksam gegen unbefugte Datenweitergabe

Teil 5: Verzeichnis der Verarbeitungstätigkeiten (10 Punkte)

1. Verantwortlicher: App-Entwicklungsfirma
2. Verarbeitungszweck: Standortdaten für personalisierte Dienste, Nutzungsstatistiken zur Verbesserung der App, Kontaktdaten für Support
3. Kategorien betroffener Personen und Daten: App-Nutzer, Standortdaten, Nutzungsdaten, Kontaktdaten
4. Empfänger oder Kategorien von Empfängern: Interne Abteilungen, externe Dienstleister
5. Löschfristen bzw. Kriterien: Standortdaten nach 6 Monaten, Nutzungsstatistiken anonymisiert nach 1 Jahr, Kontaktdaten nach Beendigung der Supportanfrage
6. Technische und organisatorische Maßnahmen: Verschlüsselung, Zugriffskontrollen, regelmäßige Schulungen