IHK Prüfungen Praxis

IHK Datenschutzbeauftragter Prüfung 2021 Praktisch

Teil A: Rechtliche Grundlagen (25 Punkte)

1. Übersicht Datenschutz-Grundverordnung (DSGVO) (8 Punkte)
a) Nennen Sie die sechs Grundprinzipien der DSGVO. (3 Punkte)
b) Erläutern Sie kurz Zweckbindung und Speicherbegrenzung. (2 Punkte)
c) Ordnen Sie folgenden Verarbeitungszwecken jeweils ein Rechtsgrundlage zu (Art. 6 DSGVO):
- Personalverwaltung in einem Industriebetrieb
- Marketing-E-Mail-Kampagne an Bestandskunden
- Kameraüberwachung von Betriebsgelände (3 Punkte)

2. Landesdatenschutzgesetz (LDSG) und BDSG-neu (5 Punkte)
a) Beschreiben Sie zwei wesentliche Unterschiede zwischen BDSG-neu und DSGVO. (2 Punkte)
b) Unter welchen Voraussetzungen schreibt das BDSG-neu einen Datenschutzbeauftragten (DSB) vor? Nennen Sie mindestens drei Kriterien. (3 Punkte)

3. Betroffenenrechte (12 Punkte)
a) Ein betroffener Kunde verlangt Auskunft nach Art. 15 DSGVO. Welche Informationen muss das Unternehmen innerhalb eines Monats liefern? Listen Sie fünf Inhalte auf. (5 Punkte)
b) Ein ehemaliger Mitarbeiter verlangt Löschung seiner personenbezogenen Daten (Art. 17 DSGVO). Prüfen Sie drei Ausnahmefälle, in denen die Löschung nicht zu erfolgen hat. (4 Punkte)
c) Wie lange darf die Bearbeitungsfrist bei komplexen Anfragen nach Art. 12 Abs. 3 DSGVO maximal verlängert werden? (1 Punkt)
d) Skizzieren Sie in einem Ablaufdiagramm (Handskizze) die Schritte zur Bearbeitung einer Auskunftsanfrage. (2 Punkte)

Teil B: Datenschutzorganisation und Prozesse (25 Punkte)

1. Verzeichnis von Verarbeitungstätigkeiten (VVT) (10 Punkte)
a) Nennen Sie fünf Mindestangaben, die in einem VVT für eine Personaldatenbank enthalten sein müssen. (5 Punkte)
b) Erstellen Sie eine tabellarische Vorlage mit folgenden Spaltenüberschriften: Zweck, Kategorien betroffener Personen, Datenkategorien, Empfänger, Löschfristen. Füllen Sie eine Zeile beispielhaft mit fiktiven Daten eines Online-Shops. (5 Punkte)

2. Datenschutz-Folgenabschätzung (DSFA) (10 Punkte)
Gegeben: Ein Krankenhaus plant den Einsatz einer KI-gestützten Diagnoseunterstützung, die patientenbezogene Gesundheitsdaten auswertet.
a) Beschreiben Sie drei Risiken für die Rechte und Freiheiten der Betroffenen. (3 Punkte)
b) Nennen Sie vier Maßnahmen zur Risikominderung und ordnen Sie jeweils technische oder organisatorische Kategorie zu. (4 Punkte)
c) In welchem Artikel der DSGVO ist die DSFA geregelt und wann ist sie durchzuführen? (3 Punkte)

3. Schulung und Sensibilisierung (5 Punkte)
a) Entwerfen Sie das Programm für eine 60-minütige Mitarbeiterschulung zum Thema Social Engineering. (4 Punkte)
b) Welchen Nachweis muss das Unternehmen über die Schulung führen? (1 Punkt)

Teil C: Technische und organisatorische Maßnahmen (30 Punkte)

1. Zugriffskontrolle (10 Punkte)
Ein Mittelstandsunternehmen organisiert den Zugriff auf Kundendaten in einer On-Premise-Datenbank.
a) Erläutern Sie mindestens drei TOMA aus Anhang I DSGVO, die hier anzuwenden sind, und ihre Wirkung. (6 Punkte)
b) Skizzieren Sie ein Berechtigungskonzept mit Rollen „Admin“, „Sachbearbeiter“ und „Auditor“. Beschreiben Sie kurz die Rechtevergabe. (4 Punkte)

2. Verschlüsselung und Pseudonymisierung (10 Punkte)
a) Erklären Sie den Unterschied zwischen Verschlüsselung und Pseudonymisierung und nennen Sie je zwei Beispiele. (4 Punkte)
b) Bei der E-Mail-Kommunikation mit externen Partnern sollen vertrauliche Daten verschlüsselt werden. Nennen Sie zwei gängige Verfahren und erläutern Sie kurz deren Funktionsprinzip. (4 Punkte)
c) Wie sind Schlüssel sicher zu verwalten? Nennen Sie drei Best Practices. (2 Punkte)

3. Backup und Wiederherstellung (10 Punkte)
a) Ein Unternehmen erstellt wöchentliche Voll-Backups und tägliche inkrementelle Backups. Berechnen Sie, wie viele Wiederherstellungspunkte nach vier Wochen vorhanden sind. (2 Punkte)
b) Welche Maßnahmen stellen sicher, dass Backups beim Angriff mit Ransomware intakt bleiben? Nennen Sie vier. (4 Punkte)
c) Entwickeln Sie ein Testverfahren, um die Wiederherstellbarkeit der Backups vierteljährlich zu prüfen. (4 Punkte)

Teil D: Fallstudie und Praxis (20 Punkte)

Fallstudie: „Musterstadtwerke GmbH“ betreibt Versorgungsnetze und plant eine App zur Verbrauchsdatenerfassung. Die App sammelt Standort, Zeitstempel, Verbrauchsdaten und Nutzerprofil.

1. Datenschutzkonzept App (8 Punkte)
a) Formulieren Sie den Verarbeitungszweck in kurzer, rechtssicherer Formulierung. (2 Punkte)
b) Erstellen Sie eine Legitimationskette für Standortdaten unter Angabe der Rechtsgrundlage. (2 Punkte)
c) Nennen Sie drei Risiken aus Nutzerperspektive und jeweils eine Gegenmaßnahme. (4 Punkte)

2. Einwilligungserklärung (6 Punkte)
a) Entwerfen Sie eine Einwilligungserklärung zur Erhebung von Verbrauchs- und Standortdaten. Achten Sie auf Freiwilligkeit, Widerrufsbelehrung und Transparenz. (5 Punkte)
b) Wie muss der Widerruf technisch umgesetzt werden, damit der Nutzer sofortige Wirkung sieht? (1 Punkt)

3. Datenschutzverletzung (6 Punkte)
Gegeben: Ein Angreifer erlangt unbemerkt Zugriff auf Verbrauchsprofile von 1.200 Endkunden.
a) Prüfen Sie, ob eine Meldung an die Aufsichtsbehörde nötig ist (Art. 33 DSGVO). Begründen Sie kurz. (3 Punkte)
b) Welche Informationen müssen Betroffene gemäß Art. 34 DSGVO erhalten? Listen Sie vier Inhalte auf. (3 Punkte)

Gesamt: 100 Punkte. Viel Erfolg!