

IHK Datenschutzbeauftragter Prüfung 2022 Praktisch

IHK-Prüfung „Datenschutzbeauftragter“ – Schriftliche Simulation (Gesamt 100 Punkte, Bearbeitungszeit 180 Minuten)

Teil 1: Rechtsgrundlagen und zentrale Begriffe (20 Punkte)

1. Definieren Sie in jeweils zwei Sätzen (je 2 Punkte)
 - a) Personenbezogene Daten
 - b) Verarbeitung
 - c) Einwilligung
2. Nennen Sie die folgenden Rechtsquellen in der korrekten Rangfolge (5 Punkte):
 - Datenschutz-Grundverordnung
 - BDSG-neu
 - Landesdatenschutzgesetze
 - EU-Grundrechtecharta
3. Unterscheiden Sie Verantwortlicher und Auftragsverarbeiter anhand der Entscheidungsbefugnisse über Zweck und Mittel der Verarbeitung (3 Punkte).
4. Erläutern Sie anhand eines Beispiels aus dem Personalwesen Zweckbindung und Speicherbegrenzung (6 Punkte).

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

Der Onlineshop TechTrend verarbeitet Kundendaten u. a. für Verkauf, Versand und Marketing.

- a) Prüfen Sie, ob die Datenerhebung von Geburtsdatum und E-Mail-Adresse für den Newsletter auf Art. 6 Abs. 1 DSGVO gestützt ist. Nennen Sie die in Frage kommenden Rechtsgrundlagen und begründen Sie Ihre Auswahl (8 Punkte).
- b) Erstellen Sie ein Löschkonzept in Form einer Tabelle mit drei Datenkategorien (Bestelldaten, Newsletter-Abonnenten, Supportanfragen) und den jeweils anzuwendenden Fristen (4 Punkte).
- c) Führen Sie eine Risikoanalyse für eine Datenpanne im Vertriebssystem durch. Beschreiben Sie mindestens drei Risiken, deren Eintrittswahrscheinlichkeit und potenzielle Schadenhöhe (6 Punkte).
- d) Berechnen Sie anhand folgender fiktiver Basisdaten (Jahresumsatz Shop: 5 Mio. €, Anteil personenbezogene Daten betroffen: 10 %) die mögliche Bußgeldhöhe nach Art. 83 DSGVO bei schwerwiegender Fahrlässigkeit (6 Punkte).
- e) Beschreiben Sie in Stichpunkten die Pflichten von TechTrend zur Meldung der Panne an die Aufsichtsbehörde und Betroffene (6 Punkte).

Teil 3: Technische und organisatorische Maßnahmen (20 Punkte)

- a) Zeichnen Sie (Skizze) die Netzwerkarchitektur eines mittelständischen Unternehmens mit DMZ, Intranet, VPN und Kennzeichnung der einzelnen Schutzebenen (6 Punkte).
- b) Beschreiben Sie schriftlich, wie Sie das 4-Augen-Prinzip in einem Dokumentenmanagementsystem umsetzen (4 Punkte).
- c) Erläutern Sie kurz die Funktionsweise von TLS und AES zur Sicherung von Datenübertragungen (5 Punkte).
- d) Entwickeln Sie ein grobes Konzept für eine Mitarbeiterschulung zum Datenschutz (Zielgruppen, Inhalte, Häufigkeit) (5 Punkte).

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

In der Firma BioSecure soll künftig ein biometrisches Zutrittssystem eingeführt werden.

- a) Beschreiben Sie den Ablauf einer DSFA in mindestens sechs aufeinanderfolgenden Schritten (8 Punkte).
- b) Erstellen Sie eine Risikomatrix (Tabelle) mit drei identifizierten Risiken (z. B. unbefugter Zugriff, Systemausfall, Datenweitergabe) und bewerten Sie jeweils Eintrittswahrscheinlichkeit und Schadensschwere (8 Punkte).
- c) Leiten Sie aus der Matrix drei technische oder organisatorische Maßnahmen ab und bewerten Sie deren Wirksamkeit (4 Punkte).

Teil 5: Verzeichnis der Verarbeitungstätigkeiten (10 Punkte)

Eine App-Entwicklung verarbeitet Standortdaten, Nutzungsstatistiken und Kontaktdaten.

Erstellen Sie für drei Verarbeitungstätigkeiten ein tabellarisches Verzeichnis mit folgenden Spalten:

1. Verantwortlicher
2. Verarbeitungszweck
3. Kategorien betroffener Personen und Daten
4. Empfänger oder Kategorien von Empfängern
5. Löschfristen bzw. Kriterien für die Festlegung
6. Technische und organisatorische Maßnahmen

Füllen Sie die Tabelle vollständig aus (10 Punkte).