IHK Datenschutzbeauftragter Prüfung 2021 Praktisch – Lösungen

Teil A: Rechtliche Grundlagen

1. Übersicht Datenschutz-Grundverordnung (DSGVO) (8 Punkte)
a) Die sechs Grundprinzipien der DSGVO sind: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. (3 Punkte)
b) Zweckbindung bedeutet, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Speicherbegrenzung besagt, dass Daten nur so lange gespeichert werden dürfen, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. (2 Punkte)
c) Personalverwaltung: Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO); Marketing-E-Mail-Kampagne: berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO); Kameraüberwachung: berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO). (3 Punkte)

2. Landesdatenschutzgesetz (LDSG) und BDSG-neu (5 Punkte)
a) Zwei wesentliche Unterschiede: BDSG-neu ergänzt die DSGVO um nationale Regelungen, z.B. für Beschäftigtendatenschutz; BDSG-neu regelt spezifische Anforderungen an Videoüberwachung. (2 Punkte)
b) Ein Datenschutzbeauftragter ist erforderlich, wenn: mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind; die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht; die Kerntätigkeit in der systematischen Überwachung von Personen besteht. (3 Punkte)

3. Betroffenenrechte (12 Punkte)
a) Informationen, die geliefert werden müssen: Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger oder Kategorien von Empfängern, geplante Speicherdauer, Bestehen eines Rechts auf Berichtigung oder Löschung. (5 Punkte)
b) Ausnahmefälle: Ausübung des Rechts auf freie Meinungsäußerung und Information, Erfüllung einer rechtlichen Verpflichtung, Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. (4 Punkte)
c) Die Bearbeitungsfrist kann um zwei Monate verlängert werden. (1 Punkt)
d) Schritte zur Bearbeitung einer Auskunftsanfrage: Eingang der Anfrage, Prüfung der Identität, Sammlung der Informationen, Erstellung der Antwort, Versand der Antwort. (2 Punkte)

Teil B: Datenschutzorganisation und Prozesse

1. Verzeichnis von Verarbeitungstätigkeiten (VVT) (10 Punkte)
a) Mindestangaben: Name und Kontaktdaten des Verantwortlichen, Zwecke der Verarbeitung, Beschreibung der Kategorien betroffener Personen, Kategorien personenbezogener Daten, Empfänger der Daten. (5 Punkte)
b) Beispiel Online-Shop: Zweck: Bestellabwicklung; Kategorien betroffener Personen: Kunden; Datenkategorien: Name, Adresse, Zahlungsdaten; Empfänger: Versanddienstleister; Löschfristen: 10 Jahre. (5 Punkte)

2. Datenschutz-Folgenabschätzung (DSFA) (10 Punkte)
a) Risiken: Verlust der Vertraulichkeit, unbefugter Zugriff auf Gesundheitsdaten, Diskriminierung durch fehlerhafte Diagnosen. (3 Punkte)
b) Maßnahmen: Verschlüsselung (technisch), Zugangskontrollen (organisatorisch), regelmäßige Schulungen (organisatorisch), Pseudonymisierung (technisch). (4 Punkte)
c) Die DSFA ist in Art. 35 DSGVO geregelt und durchzuführen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. (3 Punkte)

3. Schulung und Sensibilisierung (5 Punkte)
a) Programm: Einführung in Social Engineering, Beispiele und Techniken, Erkennung von Angriffen, Schutzmaßnahmen, Diskussion und Fragen. (4 Punkte)
b) Nachweis: Teilnahmebescheinigungen oder Schulungsprotokolle. (1 Punkt)

Teil C: Technische und organisatorische Maßnahmen

1. Zugriffskontrolle (10 Punkte)
a) TOMA: Zugangskontrolle (Verhinderung unbefugten Zugangs), Zugriffskontrolle (Verhinderung unbefugter Nutzung), Weitergabekontrolle (Verhinderung unbefugter Weitergabe). (6 Punkte)
b) Berechtigungskonzept: Admin: Vollzugriff; Sachbearbeiter: Zugriff auf Kundendaten; Auditor: Leserechte für Prüfzwecke. (4 Punkte)

2. Verschlüsselung und Pseudonymisierung (10 Punkte)
a) Verschlüsselung: Daten sind nur mit Schlüssel lesbar (z.B. AES, RSA); Pseudonymisierung: Daten sind ohne Zusatzinformationen nicht einer Person zuzuordnen (z.B. ID-Nummern, Tokenisierung). (4 Punkte)
b) Verfahren: PGP (asymmetrische Verschlüsselung), S/MIME (Zertifikatsbasierte Verschlüsselung). Beide verschlüsseln den Inhalt der E-Mail, sodass nur der Empfänger mit dem passenden Schlüssel lesen kann. (4 Punkte)
c) Schlüsselverwaltung: Verwendung von Hardware-Sicherheitsmodulen, regelmäßige Schlüsselrotation, sichere Speicherung in verschlüsselten Datenbanken. (2 Punkte)

3. Backup und Wiederherstellung (10 Punkte)
a) Nach vier Wochen: 4 Voll-Backups, 24 inkrementelle Backups. (2 Punkte)
b) Maßnahmen: Offline-Backups, regelmäßige Überprüfung der Backups, Einsatz von Anti-Ransomware-Software, Verschlüsselung der Backups. (4 Punkte)
c) Testverfahren: Wiederherstellungstest mit ausgewählten Daten, Überprüfung der Integrität, Dokumentation der Testergebnisse, Anpassung des Backup-Plans bei Bedarf. (4 Punkte)

Teil D: Fallstudie und Praxis

1. Datenschutzkonzept App (8 Punkte)
a) Verarbeitungszweck: Erfassung und Analyse von Verbrauchsdaten zur Optimierung der Energieversorgung. (2 Punkte)
b) Legitimationskette: Standortdatenverarbeitung auf Basis der Einwilligung des Nutzers (Art. 6 Abs. 1 lit. a DSGVO). (2 Punkte)
c) Risiken und Gegenmaßnahmen: Datenverlust (Verschlüsselung), unbefugter Zugriff (Zugangskontrollen), Profilbildung (Pseudonymisierung). (4 Punkte)

2. Einwilligungserklärung (6 Punkte)
a) Einwilligungserklärung: Freiwillige Zustimmung zur Erhebung von Verbrauchs- und Standortdaten, Widerrufsrecht jederzeit möglich, klare und verständliche Sprache. (5 Punkte)
b) Technische Umsetzung: Sofortige Deaktivierung der Datenerfassung und Bestätigung an den Nutzer. (1 Punkt)

3. Datenschutzverletzung (6 Punkte)
a) Meldung an die Aufsichtsbehörde ist erforderlich, da ein Risiko für die Rechte und Freiheiten der Betroffenen besteht. (3 Punkte)
b) Informationen an Betroffene: Art der Verletzung, mögliche Folgen, ergriffene Maßnahmen, Kontaktinformationen des Datenschutzbeauftragten. (3 Punkte)