IHK Datenschutzbeauftragter Prüfung 2023 Praktisch – Lösungen

Teil A: Rechtsgrundlagen (20 P)

Aufgabe A1 (8 P)
1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Daten müssen rechtmäßig, fair und transparent verarbeitet werden.
2. Zweckbindung: Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden.
3. Datenminimierung: Es dürfen nur relevante und notwendige Daten erhoben werden.
4. Richtigkeit: Daten müssen korrekt und aktuell sein.
5. Speicherbegrenzung: Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke notwendig ist.
6. Integrität und Vertraulichkeit: Daten müssen durch geeignete Sicherheitsmaßnahmen geschützt werden.

Aufgabe A2 (6 P)
a) Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO): Die Verarbeitung ist zur Erfüllung eines Vertrags erforderlich.
b) Auskunftsrecht: Der Kunde kann eine Kopie seiner verarbeiteten Daten anfordern. Recht auf Löschung: Der Kunde kann die Löschung seiner Daten verlangen, wenn sie nicht mehr benötigt werden.

Aufgabe A3 (6 P)
Bußgeld: 50 Mio EUR x 2% = 1 Mio EUR. Das Bußgeld liegt unter der Maximalbegrenzung von 10 Mio EUR, da 2% des Umsatzes weniger als 10 Mio EUR sind.

Teil B: Organisatorische Maßnahmen (20 P)

Aufgabe B1 (10 P)
Verzeichnis der Verarbeitungstätigkeiten:
1. Personalverwaltung: Zweck - Gehaltsabrechnung; Betroffene - Mitarbeiter; Daten - Name, Gehalt; Empfänger - Finanzamt; Löschfrist - 10 Jahre.
2. Marketing: Zweck - Kundenakquise; Betroffene - Kunden; Daten - E-Mail; Empfänger - Marketingagentur; Löschfrist - 2 Jahre.
3. IT-Support: Zweck - Fehlerbehebung; Betroffene - Mitarbeiter; Daten - Benutzername; Empfänger - IT-Dienstleister; Löschfrist - 1 Jahr.
4. Lieferantenverwaltung: Zweck - Bestellabwicklung; Betroffene - Lieferanten; Daten - Kontaktdaten; Empfänger - Buchhaltung; Löschfrist - 5 Jahre.
5. Kundenbetreuung: Zweck - Support; Betroffene - Kunden; Daten - Bestellnummer; Empfänger - Kundenservice; Löschfrist - 3 Jahre.

Aufgabe B2 (10 P)
Schulungs- und Kontrollkonzept:
1. Thema - Datenschutzgrundlagen; Zielgruppe - Alle Mitarbeiter; Häufigkeit - Jährlich; Verantwortlicher - Datenschutzbeauftragter; Nachweis - Teilnehmerliste.
2. Thema - IT-Sicherheit; Zielgruppe - IT-Abteilung; Häufigkeit - Bei Änderung; Verantwortlicher - IT-Leiter; Nachweis - Quiz.
3. Thema - Umgang mit Kundendaten; Zielgruppe - Kundenservice; Häufigkeit - Halbjährlich; Verantwortlicher - Abteilungsleiter; Nachweis - Teilnehmerliste.

Teil C: Technische Maßnahmen (20 P)

Aufgabe C1 (10 P)
Netzwerk-Diagramm:
- DMZ: Enthält Webserver, gesichert durch Firewall.
- Webserver: Verbindung zu Applikationsserver, gesichert durch TLS.
- Applikationsserver: Verbindung zu Datenbankserver, gesichert durch TLS.
- Datenbankserver: Interne Arbeitsplätze über VPN-Gateway erreichbar.
- Firewall: Schützt interne Netzwerke.
- VPN-Gateway: Sicherer Zugang für externe Mitarbeiter.

Aufgabe C2 (10 P)
a) Verschlüsselung ruhender Daten: Einsatz von AES-256 zur Verschlüsselung der Datenbank.
b) Pseudonymisierung: Ersetzen von Personendaten durch eindeutige Pseudonyme.
c) Protokollierung und Monitoring: Einsatz von SIEM-Systemen zur Überwachung und Protokollierung von Datenbankzugriffen.

Teil D: Datenschutz-Folgenabschätzung (20 P)

Aufgabe D1 (10 P)
Unbefugter Zugriff: A = 3, S = 5, R = 15. Datenverlust durch Fehlkonfiguration: A = 2, S = 4, R = 8.

Aufgabe D2 (10 P)
Maßnahmenplan:
1. Risiko - Unbefugter Zugriff; Maßnahme - Zwei-Faktor-Authentifizierung; Wirkung - A = 2, S = 5, R = 10; Verantwortlicher - IT-Sicherheit; Termin - Q1 2024.
2. Risiko - Datenverlust; Maßnahme - Regelmäßige Backups; Wirkung - A = 1, S = 4, R = 4; Verantwortlicher - IT-Abteilung; Termin - Q2 2024.

Teil E: Audit & Berichterstattung (20 P)

Aufgabe E1 (10 P)
Auditplan:
- Auditziele: Sicherstellung der DSGVO-Konformität.
- Prüfungsbereiche: Datenverarbeitung, IT-Sicherheit.
- Prüfmethoden: Interviews, Dokumentencheck.
- Zeitplan: Januar, Juli; Dauer: 2 Wochen.
- Verantwortliche: Datenschutzbeauftragter.

Aufgabe E2 (10 P)
Abschlussbericht:
1. Einleitung: Überblick über den Auditprozess und Ziele.
2. Methodik: Beschreibung der angewandten Prüfmethoden.
3. Ergebnisse: Zusammenfassung der wichtigsten Feststellungen.
4. Maßnahmen: Empfohlene Korrekturmaßnahmen.
5. Fazit: Bewertung der Datenschutzkonformität.
6. Anhang: Detaillierte Prüfprotokolle und Dokumentationen.