IHK Datenschutzbeauftragter Prüfung 2025 Praktisch – Lösungen

Teil A: Grundkenntnisse Datenschutzrecht

Aufgabe 1

a) „personenbezogene Daten“ (3 P)
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person gilt als identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

b) „Verantwortlicher“ vs. „Auftragsverarbeiter“ (4 P)
Der Verantwortliche ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Auftragsverarbeiter hingegen ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

c) „Einwilligung“ nach Art. 4 Nr. 11 und Art. 7 DSGVO (3 P)
Einwilligung ist jede 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. Art. 7 DSGVO spezifiziert die Bedingungen für die Einwilligung, einschließlich der Nachweispflicht des Verantwortlichen und des Rechts auf Widerruf.

Aufgabe 2

a) Auskunftsrecht (Art. 15) (5 P)
Das Auskunftsrecht ermöglicht es der betroffenen Person, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat die betroffene Person das Recht auf Auskunft über diese Daten und auf folgende Informationen: Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger, geplante Speicherdauer, Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, Beschwerderecht bei einer Aufsichtsbehörde, Herkunft der Daten und das Bestehen einer automatisierten Entscheidungsfindung. Ausnahmen können bestehen, wenn die Auskunft die Rechte und Freiheiten anderer Personen beeinträchtigen würde.

b) Recht auf Berichtigung (Art. 16) (4 P)
Die betroffene Person hat das Recht, unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

c) Recht auf Löschung („Recht auf Vergessenwerden“, Art. 17) (6 P)
Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft: Die Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig, die betroffene Person widerruft ihre Einwilligung, die Daten wurden unrechtmäßig verarbeitet, oder die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich. Ausnahmen bestehen, wenn die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich ist.

d) Widerspruchsrecht (Art. 21) (5 P)
Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen. Der Verantwortliche darf die personenbezogenen Daten dann nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Teil B: Umsetzung der DSGVO in der Praxis

Aufgabe 3

1) Auftragsverarbeiter-Vertrag (3 P)
Ein Vertrag zur Auftragsverarbeitung muss abgeschlossen werden, der die Verarbeitung im Auftrag regelt und sicherstellt, dass der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreift, um die Rechte der betroffenen Personen zu schützen.

2) Übermittlung in Drittländer (4 P)
Es müssen geeignete Garantien für die Übermittlung personenbezogener Daten in Drittländer getroffen werden, z.B. durch den Abschluss von Standardvertragsklauseln oder die Implementierung von Binding Corporate Rules.

3) Technische und organisatorische Maßnahmen (3 P)
Es sind Maßnahmen zu ergreifen, die die Sicherheit der Verarbeitung gewährleisten, wie z.B. Verschlüsselung, Pseudonymisierung, Zugangskontrollen und regelmäßige Sicherheitsüberprüfungen.

4) Nachweispflichten und Dokumentation (3 P)
Es muss eine umfassende Dokumentation der Datenverarbeitungsprozesse erstellt werden, die die Einhaltung der DSGVO nachweist, einschließlich Verarbeitungsverzeichnissen und Datenschutz-Folgenabschätzungen.

5) Schulung und Sensibilisierung der Mitarbeiter (2 P)
Mitarbeiter müssen regelmäßig geschult und für den Datenschutz sensibilisiert werden, um sicherzustellen, dass sie die Datenschutzrichtlinien und -verfahren des Unternehmens verstehen und einhalten.

Aufgabe 4

a) Fristen und Adressaten (6 P)
Eine Datenschutzverletzung muss unverzüglich und möglichst binnen 72 Stunden, nachdem sie bekannt wurde, der zuständigen Aufsichtsbehörde gemeldet werden. Wenn die Meldung nicht innerhalb von 72 Stunden erfolgt, ist eine Begründung für die Verzögerung beizufügen.

b) Inhalt der Meldung an die Aufsichtsbehörde (5 P)
Die Meldung muss mindestens folgende Informationen enthalten: die Art der Datenschutzverletzung, die Kategorien und die ungefähre Anzahl der betroffenen Personen und Datensätze, den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines anderen Ansprechpartners, die wahrscheinlichen Folgen der Datenschutzverletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und zur Minderung ihrer möglichen nachteiligen Auswirkungen.

c) Information der betroffenen Personen (4 P)
Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche die betroffenen Personen unverzüglich informieren. Die Information muss in klarer und einfacher Sprache die Art der Datenschutzverletzung, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen zur Behebung der Datenschutzverletzung beschreiben.

Teil C: Technische und organisatorische Maßnahmen

Aufgabe 5

Ein Datenflussdiagramm (DFD) sollte die folgenden Komponenten und Datenflüsse enthalten:
- Kunde: Füllt Bestellformular im Webbrowser aus.
- Webbrowser: Überträgt Daten über HTTPS an den Server.
- Server: Speichert Daten im CRM- und ERP-System.
- CRM- und ERP-System: Verarbeitet und speichert Bestelldaten.
- Versanddienstleister: Erhält Lieferadresse per API.
- Marketingabteilung: Erhält anonymisierte Verkaufsstatistik.

Aufgabe 6

1) Verarbeitung von Gesundheitsdaten im Krankenhaus (Wahrscheinlichkeit 2, Ausmaß 3)
Risikowert: 6 (hoch)

2) Speicherung von Mitarbeiterstammdaten (Wahrscheinlichkeit 1, Ausmaß 1)
Risikowert: 1 (niedrig)

3) Tracking von Webseitenbesuchern ohne Einwilligung (Wahrscheinlichkeit 3, Ausmaß 2)
Risikowert: 6 (hoch)

Teil D: Fallbeispiele und Datenschutzfolgeabschätzung

Aufgabe 7

a) Beurteilung der DSFA-Erforderlichkeit (4 P)
Eine Datenschutzfolgeabschätzung ist erforderlich, da die Videoüberwachung systematisch und umfassend öffentlich zugängliche Bereiche überwacht und ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen kann.

b) Kriterien in der DSFA (3 P)
Zu prüfende Kriterien sind: Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, Risiken für die Rechte und Freiheiten der betroffenen Personen, Maßnahmen zur Bewältigung der Risiken.

c) Konzept für Schutzmaßnahmen (3 P)
Schutzmaßnahmen könnten umfassen: Begrenzung der Überwachungsbereiche, Einsatz von Pseudonymisierungstechniken, regelmäßige Überprüfung der Notwendigkeit der Überwachung, klare Informationspflichten gegenüber den betroffenen