DSB-5seenland.de

Grundlagen der DSGVO- Auszüge aus IHK-Prüfungen IT ab 2021

Aufgabe 1

Ausgangssituation:
Die Bau GmbH & Co wählt einen Server für Sicherungsaufgaben aus. Der Server besitzt einen RAID-Controller, der RAID 5 und RAID10 unterstützt. Gem. DSGVO müssen geeignete technisch-organisatorische Maßnahmen ergriffen werden, mit denen die Schutzziele Integrität, Verfügbarkeit und Belastbarkeit bei der Verarbeitung sichergestellt werden können.
Beschreiben Sie drei Maßnahmen, die geeignet sind, die Datensicherheit beim Dateiaustausch zu gewährleisten.

Lösung:

1. Verschlüsselung über einen VPN-Tunnel
2. Redundante Internetverbindung
3. Monitoring-Tools zur Überwachung von Server und Netzkomponenten
4. Erstellen Notfallplan

Aufgabe 2

Ausgangssituation:
Bei Recherchen zur Sicherheit um das Betriebssystem hat das BSI verschiedene Empfehlungen veröffentlicht. Insbesondere „Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10".
Beschreiben Sie die besonderen Anforderungen an den Datenschutz, die bei der Protokollierung beachtet werden müssen.

Lösung:
Die Daten dürfen nur nach den Regeln der DSGVO/BDSG gespeichert und verwendet werden.
Grundsatz Datenminimierung und TOM. Z.B. zentrale Speicherung und Absicherung der Logfiles, Löschkonzept

Aufgabe 3

Ausgangssituation:
In einer Franchise-Fitnesskette mit Filialen in ganz Europa werden die personenbezogenen Daten u.a. der Mitglieder verarbeitet. Die Firmensprache ist englisch, daher wird auch die DSGVO (GDPR) auf englisch ausgelegt. Als Mitarbeiter erhalten Sie die Aufgabe, nachstehende Begriffe der GDPR auf deutsch zu interpretieren.

a) Personal data shall be processed in a transparent manner in relation to the data subject (lawfulness, fairness, and transparency)
b) Personal data shall be collected for specified explicit and legitimate purposes and no further in a manner that ist incompatible with the initial purposes (Purpose limitation)

Lösung:

a) Grundsatz Art.5,1 PbD müssen in rechtmäßiger Weise nach Treu und Glauben und für die betroffene Person nachvollziehbar verarbeitet werden. D.h. Nicht ohne Rechtsgrundlage und nicht ohne Datenschutzinformation.

b) Die PbD dürfen nur für vor der Verarbeitung festgelegte, legitime und eindeutige Zwecke verarbeitet werden und nicht auf eine Weise, die diesen Zwecken nicht entspricht.

Über die Rechtsgrundlagen a) und die Zwecke b) ist die Betroffene Person zu informieren

Aufgabe 4

Ausgangssituation:
Die Firma IT-Solution GmbH, deren Mitarbeiter im IT-Bereich Sie sind, verarbeitet personenbezogene Daten im Auftrag der Bauwo AG. Die Bauwo AG verlangt daher vom Auftragnehmer die Erstellung eines Auftragsverarbeitungsvertrages (AV-Vertrag).
Was ist ein AV-Vertrag und was muss er beinhalten?

Lösung:
Der AV-Vertrag regelt das Verhältnis zwischen Auftraggeber (Verantwortliche Stelle) und Auftragnehmer (Auftragsverarbeiter). Er verpflichtet den Verarbeiter die Daten nur nach Weisung der Verantwortlichen Stelle, nach den Vorgaben der DSGVO und unter Einhaltung der angemessenen TOM zu verarbeiten.

- Vertragsgegenstand
- Anwendungsbereich,
- Behandlung Betroffenen
- Informationspflichten
- Dauer der AV
- Verantwortlichkeiten
- Dokumentation
- Haftung und Schadenersatz
- Art der Verarbeitung und TOM
- Pflichten von AN und AG
- Subunternehmer

Aufgabe 5

Ausgangssituation:
Zur rechtmäßigen Anmeldung und Versand von Newslettern wird das Double-Opt in Verfahren empfohlen. Erläutern Sie Funktionsweise und Ziel des Verfahrens

Lösung:
Beim Double-opt-in erhält der Kunde zusätzlich zur ersten Bestätigung eine Bestätigungsmail, in der er seine E-Mailadresse rückbestätigen muss

Damit wird die Bestellung und die rechtssichere Einwilligung in die Verarbeitung der PbD eingeholt. Lt. BGH ist dies das einzige rechtssichere Verfahren.

Aufgabe 6

Ausgangssituation:
Für den zielgruppengerechten Einsatz des Newsletters sollen Tracking-Cookies eingesetzt werden.
a) Erläutern Sie den technischen Begriff Cookie

b) Nennen Sie zwei Voraussetzungen, unter denen Cookies auf der Webseite rechtssicher eingesetzt werden können

Lösung:
Cookies sind kleine Dateien, die auf dem Rechner des Empfängers installiert werden und auf die Browser und Server zugreifen können. Tracking Cookies verarbeiten PbD.

- aktive Einwilligungs- Abwahlmöglichkeit des Empfängers (Cookie-Banner)

- Informationen über Art, Funktionsweise und Lebensdauer der Cookies

Aufgabe 7

Ausgangssituation:
Dem Nutzer einer Banking-App stehen aus dem Datenschutz bestimmte Rechte zu. Nennen Sie fünf in der DSGVO garantierte Betroffenenrechte.

Lösung:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung/Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch der Verarbeitung
- Beschwerderecht bei einer Aufsichtsbehörde

Aufgabe 8

Ausgangssituation:
Im Zuge der Migration aus der Zentrale eines Bäckereibetriebes erhalten Sie eine Festplatte mit:

1. Eingescannten Originalen einer Umfrage zur Kundenzufriedenheit, die fertig ausgewertet ist und gelöscht werden kann. Sie enthält Name , Adresse, Geburtsdatum und Lieblingsfiliale, etc.
2. Rechnungen über Lieferungen an eine Hotelkette aus den letzte drei Jahren

Begründen Sie, welche der Daten gelöscht werden können und warum aus datenschutzrechtlicher Sicht das Formatieren und Löschen nicht ausreicht

Lösung:
Rechnungen haben 10 Jahre Aufbewahrungsfrist und Lieferscheine 6 Jahre. Die können also nicht gelöscht werden. Sie müssen aber dem allgemeinen Zugriff entzogen werden (Pseudonymisierung, Einschränkung Zugriffsrechte)

Nach den Formatierungs-, Löschvorgängen können die Daten mit entsprechenden Mitteln wiederhergestellt werden.

Aufgabe 9

Ausgangssituation:
Der neue Filialleiter der Bäckerei fragt Sie was er tun muss, wenn jemand unrechtmäßig Zugang zur Datenbank mit den Bonusprogrammen erlangt hat, in der Name, Adresse Kundennummer etc. gespeichert sind.

Welche Informationspflichten sind bei diesem unbefugten Zugriff zu erfüllen?

Lösung:
- Information des DSB
- Meldung an die Aufsichtsbehörde innerhalb 72 Stunden
- Information der betroffenen Personen, da aus der illegalen Nutzung Schaden entstehen kann

Aufgabe 10

Ausgangssituation:
Die Fitnessstudiokette Smartfit möchte ihre Prozesse an die heutigen Standards anpassen und initialisiert ein Projekt zur Einführung einer neuen Software für die Verwaltung ihrer Mitglieder und der angebotenen Kurse.
Im Vorfeld der Einführung des neuen Reservierungs- und Buchungssystems von Kursen und Mitgliedern bekommen Sie den Auftrag eine Risikoanalyse vorzubereiten. Beschreiben Sie drei mögliche Risiken die bei der Einführung auftreten können und entwickeln Sie für jedes Risiko eine Gegenmaßnahme.

Lösung:

Risiko	Gegenmaßnahme
Datenverlust durch Strom-/Serverausfall	Einrichtung USV; Installation RAID System
Fehlbedienung durch Personal	Schulung & Training
Offenlegung PbD durch falsche Bildschirmpositionierung	Positionierung anpassen, Bildschirm abblenden

Aufgabe 11

Ausgangssituation: Die hohen Anforderungen der DSGVO an den Schutz personenbezogener Daten sind auch beim Reservierungs- und Buchungssystem zu beachten.
Beschreiben Sie drei organisatorische Maßnahmen mit Blick auf Mitarbeiter und Prozesse, mit denen sich der Schutz dieser Daten sicherstellen lässt.

Lösung:

- Einrichtung eines geeigneten Zugangs- und Berechtigungssystems zu Rechner und System
- Verfassen einer entsprechenden Arbeitsanweisung/Richtlinie
- zentrale Passwortverwaltung und –Speicherung
- Mitarbeiterschulung/Verpflichtung auf das Datengeheimnis (Vertraulichkeitsverpflichtung)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

Aufgabe 12

Ausgangssituation: Die Geschäftsleitung von Smartfit möchte durch die Einrichtung einer Webseite Interessenten und Mitglieder über das Internet erreichen. Dabei weist der DSB darauf hin, dass die Bereitstellung einer Webseite auf jeden Fall zur Verarbeitung von personenbezogenen Daten der Webseitenbesucher führen wird.
Nennen Sie eine Datenkategorie, die beim Aufruf der Webseite auf jeden Fall vom Server verarbeitet werden muss um die Webseite an den Client auszuliefern und die ein personenbezogenes Datum darstellt

Lösung:
-IP-Nr.

Aufgabe 13

Ausgangssituation: Ihr Ausbildungsbetrieb, die AMAG MED GmbH ist spezialisiert auf digitale Lösungen für die Gesundheitsbranche und managt die digitalen Prozesse eines medizinischen Pflege- und Versorgungszentrums (MPVZ). 25 Mitarbeiter des MPVZ haben Zugriff auf die Patientendaten und müssen diese elektronisch speichern und versenden. Übersendung und Speicherung von Patientendaten können aus datenschutzrechtlichen Gründen nicht im Klartext erfolgen. Es muss ebenfalls sichergestellt sein, dass kein Unbefugter Zugriff auf die Daten hat. Sie sollen das MPVZ in dieser Richtung beraten.

a) Erläutern Sie, warum Patientendaten gem. DSGVO besonders behandelt werden müssen
b) Beschreiben Sie, welche Vorgaben der DSGVO in Bezug auf die Patientendaten beachtet und umgesetzt werden müssen

Lösung:

a) Patientendaten gehören zu den besonders schützenswerten/sensiblen Daten des Art. 9 der DSGVO

b) Benennung eines DSB, Vorabkontrolle der zu übersendenden Daten (Zweckbindung, Datenminimierung)

Aufgabe 14

Ausgangssituation: Für Abmeldung am Arbeitsplatz des MPVZ soll eine Zwei-Faktor Authentifizierung eingesetzt werden. Erläutern Sie den Begriff und nennen Sie zwei konkrete technische Möglichkeiten .

Lösung:

a) Um Zugang zum Rechner zu erhalten, muss ein zweiter Faktor eingesetzt werden. Der erste Faktor soll in jedem Fall Wissen sein (Benutzerkennung &Passwort), der zweite kann aus dem Bereich Besitz oder Biometrie kommen.

b) Technische Möglichkeiten:

- Authenticator App, Token etc. (Besitz);
- Fingerabdruck, Iris-scan, Stimme etc (Biometrie)

Aufgabe 15

Ausgangssituation: Mit dem Aufbau des Systems müssen auch die drei relevanten Schutzziele des BSI-Grundschutzes erfüllt werden.

a) Nennen sie die drei Schutzziele des BSI-Grundschutzes
b) Erläutern Sie eines der Schutzziele anhand von drei Aspekten

Lösung:

a) Das sind die gemeinsamen Schutzziele aus Grundschutz & Datenschutz Vertraulichkeit, Verfügbarkeit, Integrität

b) **Vertraulichkeit:** Informationen sind nur für Befugte zugänglich, niemand kann unbefugt Informationen gewinnen, Inhalte können verschlüsselt werden;

Verfügbarkeit: technische Verfügbarkeit der Systeme, SLA, Verarbeitung muss auch korrekt ablaufen;

Integrität: keine unbefugte/unbemerkte Veränderung von Daten, Korrektheit von Daten (Datenintegrität), Funktionsweise des Systems (Systemintegrität), Wenn Manipulation nicht zu verhindern ist, darf sie nicht unbemerkt bleiben.

Aufgabe 16

Ausgangssituation: In einer Arztpraxis soll der IT-Dienstleister IT.SYS. GmbH das veraltete Mailsystem austauschen und die Daten in das neue System migrieren. Mit dem Auftraggeber wird diskutiert, ob einige Arbeiten remote durchgeführt werden sollten. Nennen Sie zwei Vorteile und zwei Nachteile der remote Lösung gegenüber vor Ort Arbeiten

Lösung:

Vorteile:

- geringere Kosten,
- Schonung interner Ressourcen,
- Kontaktvermeidung

Nachteile:

- Risiko im Bereich Datenschutz, da Zugriff auf Patientendaten möglich ist,
- zusätzliche Kosten für gesicherte Verbindung,
- keine Wartung bei Verbindungsproblemen möglich.

Aufgabe 17

Ausgangssituation: Bei einem Unternehmen soll, um einen reibungslosen Support zu gewährleisten, ein Ticketsystem auf einem Webserver installiert werden. Um die Datensicherheit und den Datenschutz zu garantieren, soll der Webserver durch ein SSL-Zertifikat gesichert werden. Erläutern Sie drei Sicherheitsmechanismen, die durch das SSL-Zertifikat erreicht werden.

Lösung:

- Einsatz von SSL-Zertifikaten ist einfach und kostengünstig
- Sender und Empfänger sind authentifiziert
- Integrität der Daten wird sichergestellt
- Zugangskontrolle ist gesichert

Aufgabe 18

Ausgangssituation: Bei einer Videoüberwachung des Aussengeländes eines Betriebs müssen die Regeln der DSGVO beachtet werden. Erläutern Sie in diesem Zusammenhang die Begriffe Löschfristen, Persönlichkeitsrecht, und Zweckbindung

Lösung:

- Löschfristen: Daten müssen gelöscht werden, wenn der Zweck erfüllt ist und/oder die Rechtsgrundlagen entfällt (z.B. Widerruf Einwilligung/Widerspruch /Löschbegehren nach Art17- Recht auf Vergessenwerden). Im VVT müssen diese Verarbeitungen die vorgesehenen Löschfristen – hier i.d.R 72 Std .- dokumentiert sein.

- Für Bild- und Videoaufnahmen ist die Einwilligung des Personals nach Art. 7 erforderlich. Möglichst im double Opt-In Verfahren

- Zweckbindung: Videoaufnahmen können präventiv sein (ohne Speicherung) oder zur Beweissicherung gespeichert werden. Darüber muss auf der Hinweistafel informiert werden. Nach der Zweckerfüllung sind die Daten zu löschen

Aufgabe 19

Ausgangssituation: Bei der Nutzung Ihres firmeneigenen Laptops als heimbasierten Telearbeitsplatz ist es u.a. wichtig, die Sicherheit der Kundendaten zu gewährleisten. Dazu werden Umsetzungshinweise zur Verfügung gestellt.

a. Nennen Sie dazu zwei in Deutschland relevante Grundlagen.
b. Nennen Sie Beispiele für sinnvolle technisch-organisatorische Maßnahmen zu folgenden Bereichen:Zutrittsschutz Telearbeitsplatz, Sichere Anmeldung am Laptop, Sichere Datenkommunikation, Transport von Datenträgern

Lösung:

a. **Grundlagen**: BDSG, DSGVO, TTDSG, Grundgesetz Art 10 (Fernmeldegeheimnis), Landesdatenschutzgesetze.

b. **TOMs:**

- **Zutrittsschutz Telearbeitsplatz:** Sicherer Raum, Türen/Fenster schließen
- **Sichere Anmeldung am Laptop:** 2F-Auth., Sicheres Passwort
- **Sichere Datenkommunikation:** VPN, Protokolle, Zugriffszeiten
- **Transport von Datenträgern**: berechtigte Person, Schulung Kuriere, Sichere Transportbehälter, Verschlüsselung

Aufgabe 20

Ausgangssituation: Am mobilen Arbeitsplatz kann es zu Nutzungskonflikten und Sicherheitsrisiken zwischen dem Mitarbeiter der Jürgen Spohn KG und im gleichen Haushalt lebenden Personen kommen. Nennen Sie zwei Nutzungskonflikte, bzw. Sicherheitsrisiken und nennen Sie jeweils eine Maßnahme zur Behebung

Lösung:

Konflikt/Risiko	Maßnahme zur Behebung
Geteilte Internet-verbindung kann zum Mitlesen des Datenverkehrs führen	• Anschaffung eines zweiten Internetzugangs • Trennung des Datenverkehrsdurch Sim-Karte
Unberechtigter Notebookzugriff durch andere Personen	• Sichere Aufbewahrung des Notebooks • Verschlüsselung • Abmeldung beim Verlassen