EXIN Privacy & Data Protection

PRACTITIONER

Certified by EXIN

Musterexamen

Ausgabe 201809

Inhalt

Einführung

Dies ist das Musterexamen EXIN Privacy & Data Protection Practitioner (PDPP.DE). Es gelten die EXIN Examen Regeln und Vorschriften.

Dieses Examen erfolgt im Multiple-Choice-Verfahren und umfasst 40 Fragen. Von den pro Frage gegebenen Antworten ist jeweils nur eine richtig.

Die maximal erreichbare Punktzahl beträgt 40 Punkte. Jede richtige Antwort zählt 1 Punkt. Das Examen gilt als bestanden, wenn ein Kandidat 26 oder mehr Punkte erreicht hat.

Die Dauer des Examens ist 120 Minuten.

Es ist erlaubt, die Datenschutz-Grundverordnung einzusehen.

Viel Erfolg!

Musterexamen

1 / 40
Welches Dokument muss der Verantwortliche betroffenen Personen zur Verfügung stellen?

A) Datenschutzpolitik
B) Richtlinie zur fairen Nutzung
C) Richtlinie zum Zugriffsmanagement
D) Richtlinie zur Informationssicherheit

2 / 40
Was muss eine gute Datenschutzpolitik aus Unternehmenssicht leisten?

A) Sie sorgt für den nötigen Datenschutz im Einklang mit Produktivität.
B) Sie definiert Ansprechpartner und Zuständigkeiten.
C) Sie erklärt, wie mit Verstössen umzugehen ist.
D) Sie erklärt die Notwendigkeit einer Datenschutzpolitik.

3 / 40
Warum ist laut DSGVO die Wahrung von Datenschutz und Privatsphäre durch datenschutzfreundliche Voreinstellungen ein Grundprinzip des Datenschutzes?

A) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass jeweils nur die personenbezogenen Daten verarbeitet werden, die für den festgelegten Zweck erforderlich sind.
B) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass personenbezogene Daten nur entsprechend der Datenschutzpolitik erhoben werden.
C) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass die betroffenen Personen die standardmässige Datenschutzpolitik akzeptieren, bevor personenbezogene Daten verarbeitet werden.

4 / 40
Ein Unternehmen startet ein Projekt zur Erstellung eines neuen kostenlosen Services für Verbraucher.

Wann ist der **beste** Zeitpunkt, um die Themen Privatsphäre und Datenschutz anzusprechen?

A) Datenschutz muss in der Umsetzungsphase des Projekts besprochen und umgesetzt werden.
B) Privatsphäre und Datenschutz müssen ab dem Start des Projekts gefördert werden.
C) Bei allen Projekten mit personenbezogenen Daten ist vor Projektabschluss ein Datenschutzaudit durchzuführen.
D) Da dieses Projekt darauf abzielt, einen kostenlosen Service für Verbraucher zu schaffen, muss der Datenschutz auf einer aktuellen Datenschutzerklärung beruhen.

5 / 40
Eine Organisation plant den Aufbau einer neuen Abteilung. Als Dienstleister soll diese betroffenen Personen die Möglichkeit bieten, ihre personenbezogenen Daten so zu speichern, dass die Datenü bertragbarkeit zwischen verschiedenen Verantwortlichen erleichtert wird. Der CEO der Organisation bittet sie um Ihren Rat.

Warum sollte ein Datenschutzmanagementsystem (DSMS) umgesetzt werden?

A) Ein DSMS trägt dazu bei wichtige Daten in ein System zu bringen.
B) Ein DSMS hilft bei der Erhebung der zu übertragenden Daten und beim Verfassung einer Sicherheitspolitik.
C) Ein DSMS verbessert das Datenmanagement und senkt die Risiken für Daten und Informationssysteme.
D) Ein DSMS ist laut DSGVO verpflichtend.

6 / 40
Warum sollte in der Vorbereitung zur Einführung eines Datenschutzmanagementsystems (DSMS) Datenvoraudits und -bewertungen durchgeführt werden?

A) Sie identifizieren Risiken in den Bereichen Datenschutz und Privatsphäre, Risiken für Einzelpersonen und Konformität (Compliance) sowie weitere Risiken, die die Organisation betreffen.
B) Sie bieten einen klaren Überblick über den Datenfluss innerhalb und ausserhalb der Organisation und ermöglichen dem Aufsichtsgremium damit, diese Datenflüsse zu bewerten.
C) Sie analysieren die Bereitschaft und das Bewusstsein des Vorstands, der Geschäftsführung und der Mitarbeiter für Datenschutz und Privatsphäre.
D) Sie bieten eine Bestandsaufnahme, wo sich die verschiedenen Arten von Daten innerhalb der Organisation befinden und wer diese Daten innerhalb der Organisation besitzt.

7 / 40
Sie sind der neue Konzerndatenschutzbeauftragte des Unternehmens ABC. Der CEO sorgt sich über den Mangel an ordnungsgemässen Kontrollen zum Schutz der Daten, die innerhalb des Unternehmens, aber auch zwischen dem Unternehmen und externen Parteien erhoben, genutzt und offengelegt werden. Sie empfehlen dem CEO die Umsetzung eines Datenschutzmanagementsystems (DSMS)

Warum spielt die Bestandsaufnahme der Datenflüsse in dieser Phase eine wesentliche Rolle?

A) Um zu ermitteln, wie die Mitarbeiter zu Fragen des Datenschutzes stehen.
B) Um sich einen klaren Überblick zu verschaffen, welche Risiken bezüglich Datenschutz und Wahrung der Privatsphäre reduziert werden müssen.
C) Um Situationen zu identifizieren, in denen Mitarbeiter ihre privaten Angelegenheiten mit offiziellen Unternehmensangelegenheiten vermischen.
D) Um das Bewusstsein der Mitarbeiter für Fragen des Datenschutzes und der Privatsphäre bei ihrer Arbeit zu stärken.

8 / 40
Was ist für die Umsetzung der organisatorischen Strukturen und Mechanismen erforderlich, die mit der Einführung der Phase 2 „Organisation von Datenschutz und Privatsphäre“ eines Datenschutzmanagementsystems (DSMS) einhergehen?

A) Die Auditierung der Massnahmen und Kontrollen im Bereich Privatsphäre und Datenschutz zur Identifizierung eventueller Lücken und Fehler.
B) Das Denken an Datenschutz und Privatsphäre muss im gesamten Unternehmen verankert werden, um Bewusstsein für Datenschutz und Privatsphäre zu schaffen.
C) Die Mitarbeiter müssen über den Stand des Datenschutz- und Privatsphärenprogramms informiert sein, um die Anforderungen des DSMS erfüllen zu können.
D) Regelmässige Meldungen an die obere Geschäftsführung, damit diese sich mit der Leistung des Datenschutzprogramms auseinandersetzt und diese fördert.

9 / 40
Das Datenschutzprogramm ist in der Datenschutzerklärung des Unternehmens verankert.

Welcher Aspekt ist hinsichtlich der Datenschutzerklärung **nicht** wichtig?

A) Die ordnungsgemässe und wirksame Anpassung an die Mission des Unternehmens.
B) Die Erarbeitung der Aufgaben, Pflichten und Rollen der mit den Datenschutzpraktiken betrauten Personen.
C) Die detaillierte Beschreibung der Strategien zur Wahrung von Datenschutz und Privatsphäre
D) Die Betonung, wie viel Wert das Unternehmen auf Datenschutz und Privatsphäre legt.

10 / 40
Einer der entscheidendsten Faktoren für eine erfolgreiche Umsetzung des Datenschutzprogramms im Unternehmen ist die Unterstützung seitens der oberen Geschäftsführung.

Was ist **kein** Zeichen für die Unterstützung des Datenschutzprogramms seitens der oberen Geschäftsführung?

A) Die Information an die Mitarbeiter, wie wichtig Datenschutz und Privatsphäre sind
B) Die Übertragung der Verantwortung und Zuständigkeit für Initiativen im Bereich Datenschutz und Privatsphäre an den Datenschutzbeauftragten und die Prozessverantwortlichen.
C) Die Bereitstellung finanzieller Mittel zur Unterstützung von Aktivitäten in den Bereichen Datenschutz und Privatsphäre.

11 / 40
Im Rahmen eines Datenschutzprogramms hat es sich bewährt, ein Datenklassifikationssystem zu erstellen, um zu sehen, welches Mass an Schutz für personenbezogene Daten erforderlich ist.

Was ist der **primäre** Zweck eines Datenklassifikationssystems?

A) Die entsprechende Kennzeichnung der unterschiedlichen Datenkategorien zu ermöglichen
B) Die Umsetzung angemessener Kontrollen im Bereich Datenschutz und Privatsphäre für unterschiedliche Datenkategorien zu ermöglichen
C) Der Schutz aller verarbeiteten Daten sicherzustellen
D) Den Zugriff auf verschiedene Datenkategorien per Zielgruppe zu beschränken

12 / 40
Sie wurden als Datenschutzbeauftragter (DSB) eines globalen Unternehmens eingestellt. Eine ihrer ersten Aufgaben besteht darin, für das Unternehmen eine Reihe von Strategien, Plänen und Richtlinien für den Datenschutz und die Privatsphäre zu entwickeln und umzusetzen.

Was sollten Sie in Phase 3 „Entwicklung und Umsetzung von Datenschutz und Privatsphäre“ als **erstes** tun?

A) Sie sollten die Bedürfnisse und Anforderungen Ihres Unternehmens im Bereich Datenschutz analysieren und definieren.
B) Sie sollten das Wissen und Verstehen der Mitarbeiter hinsichtlich der Begriffe des Datenschutzes und der Privatsphäre einschätzen.
C) Sie sollten die Best Practices der Branche recherchieren und auf Ihr Unternehmen anpassen.
D) Sie sollten die allgemeine Datenschutz- und Privatsphärenlandschaft verstehen.

13 / 40
Eine der wichtigsten Anforderungen der DSGVO ist, dass ein Unternehmen Konformität (Compliance) nachweisen muss.

Welche Phase des Datenschutzmanagementsystems (DSMS) ist aus dieser Perspektive betrachtet am **wichtigsten**?

A) Phase 1, in der die Organisation auf den Datenschutz vorbereitet wird
B) Phase 2, in der die für den Datenschutz erforderlichen organisatorischen Strukturen und Mechanismen eingeführt werden
C) Phase 3, in der Datenschutzmassnahmen der Organisation entwickelt und umgesetzt werden
D) Phase 4, in der die Governance-Mechanismen für den Datenschutz der Organisation eingeführt werden

14 / 40
Sie sind Datenschutzbeauftragter und werden gebeten, zur Datenschutz-Governance beizutragen. Sie entscheiden, dass Ihr Unternehmen betroffenen Personen Datenschutzhinweise bereitstellen sollte, die die betroffenen Personen darüber informieren, wie ihre Daten verarbeitet werden und welche Kontrollen existieren.

Was sollten diese Datenschutzhinweise **nicht** enthalten?

A) Wie die Daten erhoben, genutzt, gepflegt, aufbewahrt und offenbart werden
B) Welche personenbezogenen Daten erhoben werden
C) Welche Sicherheitsrichtlinien die Organisation umsetzt
D) Welche konkreten Kontrollen die betroffenen Personen nutzen können

15 / 40
Sie sind Datenschutzbeauftragter (DSB) in einem Beratungsunternehmen und müssen ein Incident Management System umsetzen.

Was würde ein solches System beinhalten?

A) Die Erfassung aller verarbeiteten Daten und deren Aufbewahrung an einem sicheren Ort, damit sie im Falle eines Incidents (Vorfalls) abgerufen und die zu ergreifenden Massnahmen auf ein Minimum reduziert werden können
B) Das Erkennen von Incidents, die Reaktion auf unmittelbare und langfristige Belange, die Verfolgung der Vorfälle, um die Wirksamkeit der ergriffenen Massnahmen sicherzustellen
C) Die Registrierung aller Incidents und die Durchführung einer Datenschutzfolgeabschätzung zur Analyse der Risiken und Aufstellung eines Verbesserungsplans
D) Die Registrierung aller Incidents und ihre Meldung an das Aufsichtsgremium zur Bewertung der Datenflüsse und Verbesserung der vom Aufsichtsgremium geforderten Sicherheitspolitik

16 / 40
Ein Gesundheitsinstitut arbeitet eng mit zwei anderen Gesundheitsinstituten zusammen, um eine mobile Anwendung zur Patientenüberwachung zu entwickeln. Die Institute entscheiden sich, die Ergebnisse der neuen mobilen Anwendung mit Hilfe einer Pilotanwendung zu prüfen. Bei dieser Pilotanwendung geben Ärzte und Patienten ihre personenbezogenen Daten und Qualifikationen sowie medizinische Daten in die mobile Anwendung ein. Im Rahmen des Pilotverfahrens wird eine Sicherheitsprüfung durchgeführt. Die Testergebnisse zeigen, dass die mobile Anwendung alles andere als sicher ist. Sie kann leicht gehackt und Patientendaten dann geändert werden. Ausserdem ist es möglich, dass Hacker die Rolle des Arztes übernehmen und die medizinischen Daten der Patienten ändern.

Was sollte der von den drei Gesundheitsinstituten ernannte Datenschutzbeauftragte (DSB) im Interesse der betroffenen Personen tun?

A) Der DSB muss nichts tun, da es sich nur um eine Pilotanwendung handelt, an der nur ein relativ kleiner Teil der Patientenpopulation teilnimmt.
B) Der DSB muss nichts tun, da es sich lediglich um eine Pilotanwendung handelt und daher kein hohes Risiko besteht, dass die Auswirkungen der entdeckten Schwachstellen tatsächlichen eintreten.
C) Der DSB muss die beteiligten Patienten und Ärzte informieren, da das Testergebnis für diese wahrscheinlich ein hohes Risiko beinhaltet. Darüber hinaus meldet er das Ergebnis auch an die Aufsichtsbehörde.
D) Der DSB nutzt den Testbericht, um die Sicherheitsrisiken an die für die mobile Anwendung erforderlichen Sicherheitsstandards anzupassen und informiert die Überwachungsbehörde.

17 / 40
Was ist das **wichtigste** Argument für Sie, eine externe Partei mit der Durchführung von Datenschutzbewertungen zu betrauen?

A) Um zu sehen, ob Ihre Datenschutzaktivitäten den in der Branche üblichen Standards entsprechen
B) Um eine unabhängige Validierung Ihrer Konformität (Compliance) mit den internen Datenschutzrichtlinien und geltenden rechtlichen Anforderungen zu erhalten
C) Um die Glaubwürdigkeit Ihres Datenschutzprogramms zu verbessern
D) Um Zeitdruck und Budgetzwängen zu begegnen, die in Ihrem Datenschutzprogramm eine wichtige Rolle spielen

18 / 40
In einem Unternehmen kam es gerade zu einer Verletzung des Schutzes personenbezogener Daten, die das Customer Relationship Management (CRM) System über zwei Stunden lahmgelegt hat. Als Datenschutzbeauftragter (DSB) des Unternehmens entschliessen Sie sich unter anderem eine ad hoc Datenschutzbewertung durchzuführen.

Was ist eines der **wichtigsten** Ziele einer solchen unangekündigten Bewertung?

A) Beratung für eine entsprechende Benachrichtigung der Kunden zu geben
B) Bewertung des Ausmasses des Schadens, der durch die Verletzung des Schutzes personenbezogener Daten verursacht wurde
C) Ermittlung der Risiken für den Datenschutz
D) Identifizierung der für die Verletzung des Schutzes personenbezogener Daten verantwortlichen Personen

19 / 40
Ein Unternehmen, das gleichzeitig Verantwortlicher für die Datenverarbeitung ist, kämpft seit einiger Zeit mit finanziellen Schwierigkeiten. Der Vorstand beschliesst, die Software des Datenschutzmanagementsystems (DSMS) nicht zu aktualisieren. Stattdessen bittet das Unternehmen die Aufsichtsbehörde, die Anwendung einer Datenschutzzertifizierung zu genehmigen. Dies spart dem Unternehmen viel Geld und bringt ihm wirtschaftlichen Mehrwert.

Sie sind der Datenschutzbeauftragte (DSB) dieses Verantwortlichen, welchen Rat sollten Sie dem Vorstand geben?

A) Das Verfahren zu verfolgen und die Datenschutzzertifizierung zu erwerben. Mit dem Zertifikat kann das Unternehmen nachweisen, dass es seine Pflichten als Verantwortlicher erfüllt.
B) Die Durchführung einer externen Datenschutzbewertung. Durch diese Massnahme wird zwar das gesamte Budget erschöpft, es wird aber auch sichergestellt, dass die technischen und organisatorischen Massnahmen ergriffen werden, die der Art, dem Umfang und dem Kontext der personenbezogenen Daten entsprechen.
C) Die Software des DSMS nur zu einem Drittel zu aktualisieren, wobei nur jene Teile aktualisiert werden, die laut einer internen Bewertung die meisten Sicherheitslücken aufweisen und aktualisiert werden mü ssen.
D) Das DSMS zu aktualisieren. Die Nichtaktualisierung des DSMS führt zu einem potenziellen Risiko der Nichtkonformität. Dies kann als Nichtdurchführung geeigneter technischer und organisatorischer Massnahmen seitens des Verantwortlichen gewertet werden.

20 / 40
Ein beliebter Fitness-Club im Zentrum von Paris speichert seine Daten bei einem ebenfalls in Paris ansässigen Hosting-Unternehmen. Die Server, auf denen die Daten der Mitglieder des Fitnessclubs gespeichert sind, wurden vor kurzem von einem IT-Serviceunternehmen im Rahmen der regulären Instandhaltung überprüft. Am Tag nach dem Besuch des IT-Serviceunternehmens fällt der Server aus und verursacht einen Brand im Serverraum. Die Daten des Fitness-Clubs und deren Backups, die auf dem gleichen Server gespeichert waren, gehen bei dem Brand verloren. Eine Untersuchung ergibt, dass das Kühlsystem im Serverraum nicht gut funktionierte und das Überhitzen des Serversystems verursacht hat. Dem Instandhaltungstechniker war aufgefallen, dass die Temperatur im Raum ein wenig hoch war. Er hat dies aber nicht an das Serverunternehmen gemeldet, da er in Eile war und diesen Umstand nicht besonders aussergewöhnlich fand. Das Kühlsystem wird von dem Hostingunternehmen selbst gewartet.

Welche Partei ist am **wahrscheinlichsten** für den Vorfall verantwortlich?

A) Der Fitness-Club, weil die Organisation für die verlorenen Daten verantwortlich ist
B) Der Fitness-Club, weil er nicht angeordnet hat, dass die Backups auf einem anderen Server gespeichert werden müssen
C) Das Hostingunternehmen, weil dieses für die Sicherheit rund um die personenbezogenen Daten verantwortlich ist
D) Das IT-Unternehmen, da der Instandhaltungstechniker hätte melden müssen, dass die Temperatur im Serverraum ziemlich hoch ist

21 / 40
Ein Krankenhaus hat das Ausdrucken seiner Patientenrechnungen an eine Druckerei ausgelagert. Die Druckerei druckt auch Rechnungen für andere Unternehmen. Aufgrund einer Verwechslung von Namen und Adressen beim Sortieren in der Druckerei wurden einige Rechnungen an die falschen Patienten geschickt. Das Krankenhaus hatte seine Geschäfte sorgfältig analysiert. Das Krankenhaus verfügte über einen sehr robusten Verifizierungsprozess und vertragliche Vereinbarungen mit den Druckereien.

Warum ist die Druckerei wahrscheinlich haftbar?

A) Weil sie den Zweck der Auftragsverarbeitung bestimmt.
B) Weil sie die Druckverfahren bestimmt.
C) Weil sie bestimmt, welche Daten verarbeitet werden.
D) Weil sie auch Abrechnungen für andere Organisationen druckt.

22 / 40
Ein inhabergeführtes Haushaltwarengeschäft entschliesst sich, ein Website-Analyse-Unternehmen mit gezielter Werbung und Marketing zu beauftragen. Der Arzt und der Rechtsanwalt im gleichen Ort entschliessen sich ebenfalls, das gleiche Website-Analyse-Unternehmen zu beauftragen, das daneben noch andere Kunden hat.

Welche Organisation(en) müssen einen Datenschutzbeauftragten (DSB) bestellen?

A) Das inhabergeführte Haushaltswarengeschäft
B) Das inhabergeführte Haushaltswarengeschäft und das Website-Analyse-Unternehmen
C) Der Arzt und der Rechtsanwalt
D) Das Website-Analyse-Unternehmen

23 / 40
Auf der Insel Texel, einer kleinen Insel in der Nordsee, die zu den Niederlanden gehört, lebt ein Hausarzt. Er führt ein privates, gewinnorientiertes Unternehmen. Seine Arztpraxis hat 60 registrierte Patienten

Welche Aussage bezüglich der Bestellung eines Datenschutzbeauftragten (DSB) ist korrekt?

A) Die Arztpraxis ist zu klein und gilt daher nicht als Praxis, die in grossem Umfang für medizinischen Daten verantwortlich ist beziehungsweise diese verarbeitet. Daher muss der Hausarzt keinen DSB bestellen.
B) Die Arztpraxis überwacht regelmässig und systematisch Patienten. Deshalb muss der Arzt einen DSB bestellen.
C) Der Hausarzt betreibt die einzige Arztpraxis auf der Insel. Er übt hinsichtlich seiner Patienten eine unabhängige und professionelle Rolle aus. Er kann Arzt und DSB in Personalunion sein.

24 / 40
Laut der Datenschutzgrundverordnung (DSGVO), ist der Datenschutzbeauftragte (DSB) hinsichtlich der Ausübung seiner Tätigkeiten zur Vertraulichkeit und Geheimhaltung verpflichtet.

Welche Partei kann der DSB für Ratschläge konsultieren und ist in diesem Zusammen von seiner Pflicht zur Vertraulichkeit und Geheimhaltung entbunden?

A) Den Vorstand des Unternehmens
B) Die Mitglieder des Datenschutzteams
C) Den Informationssicherheitsbeauftragten (ISB)
D) Die Aufsichtsbehörde

25 / 40
Sie sind als Datenschutzbeauftragter (DSB) für eine Kaufhauskette im Bereich der Luxusmode tätig. Das Unternehmen hat die Absicht geäussert, eine Gesichtserkennungssoftware erwerben zu wollen, um seine Stammkunden besser identifizieren und bedienen zu können. Alle Kunden, die ein Konto bei der Kaufhauskette haben, sollen über die Änderung informiert werden und erhalten die Möglichkeit zum Opt-Out.

Warum sollten Sie vorab die Durchführung einer Datenschutzfolgeabschätzung (DPIA) empfehlen?

A) Eine Datenschutzfolgeabschätzung ist laut ISO 27001 ein wesentlicher Bestandteil eines Informationssicherheitssystems (ISMS).
B) Die Durchführung einer Datenschutzfolgeabschätzung und deren Unterzeichnung seitens der Geschäftsführung gehört zur guten Praxis, damit das Unternehmen nicht für künftige Zwischenfälle im Bereich der IT-Sicherheit haftbar gemacht werden kann.
C) Laut der DSGVO ist die Durchführung einer Datenschutzfolgeabschätzung verpflichtend, wenn neue Technologien eingesetzt werden, die sich durch Profiling oder Massenüberwachung auf den Schutz der personenbezogenen Daten auswirken können.
D) Laut der DSGVO ist bei jeder Änderung der bestehenden Prozesse, Projekte oder Richtlinien eine Datenschutzfolgeabschätzung erforderlich.

26 / 40
Stellen Sie sich vor, Sie arbeiten für eine grosse Organisation. Ihre Organisation nutzt Software-Tools, mit denen die Mitarbeiter hinsichtlich ihrer Arbeit am Computer leichter überwacht werden können. Die Tools zeigen basierend auf allgemeinen Algorithmen und Zeitangaben an, wann die Mitarbeiter eine Ruhepause benötigen oder sich dehnen sollten. Jetzt will das Unternehmen das Tool um eine Funktionalität erweitern und es an einen Pulsmesser anschliessen, um die Ratschläge bezüglich der Ruhepausen noch besser personalisieren zu können.

Warum müssen Sie eine Datenschutzfolgeabschätzung (DPIA) durchführen?

A) Eine Datenschutzfolgeabschätzung ist bei allen neuen Tools oder Prozessen erforderlich.
B) Das Tool überwacht die Mitarbeiter und umfasst damit die Verarbeitung personenbezogener Daten
C) Es handelt sich um eine neue Anwendung bei der sensible personenbezogene Daten verarbeitet werden.
D) Es handelt sich um eine neue Anwendung mit umfangreicher Überwachung des Verhaltens im öffentlichen Raum.

27 / 40
Sie haben gerade Ihren neuen Job als leitender Datenschutzbeauftragter (DSB) im nationalen Verkehrsministerium angetreten. Das Ministerium gibt ein neues Projekt bekannt, das darauf abzielt, das Fahrverhalten der Bürger auf den nationalen Schnellstrassen zu überwachen. Das Ministerium plant den Einsatz eines intelligenten Videoanalysesystems, das automatisch die Nummernschilder einzelner Fahrzeuge erkennt. Eines Morgens kommt die Staatssekretärin in Ihr B üro. Sie will offensichtlich schnell mit dem Projekt beginnen und äussert ihre Sorgen dass Datenschutzfragen zu nicht erwünschten Verzögerungen führen könnten

Was sollten Sie ihr sagen?

A) Sie sollten sie bitten, sich an die Aufsichtsbehörde zu wenden, da dies eine Frage von nationaler Bedeutung ist, die Ihre Befugnisse ganz klar übersteigt.
B) Sie sollten sie darüber informieren, dass die Art der geplanten Datenverarbeitung, eine Untersuchung mittels Durchführung einer Datenschutzfolgeabschätzung (DPIA) erforderlich macht. Die sich ergebenden Risiken und die Massnahmen zur Verringerung dieser Risiken sollten in den Projektplan integriert werden.
C) Sie informieren sie, dass keine Notwendigkeit für eine Datenschutzfolgeabschätzung (DPIA) besteht, vorausgesetzt die Bürger werden ordnungsgemäss über den Zweck und den Umfang der Datenverarbeitung informiert.
D) Sie sagen ihr, dass das Projekt ernsthaft überdacht werden sollte, da Aktivitäten zur Datenverarbeitung mit 'hohem Risiko' wie Massenüberwachung und Datenverarbeitung zur Erstellung von Profilen laut der DSGVO verboten sind.

28 / 40
Die DSGVO spezifiziert lediglich, dass eine Datenschutzfolgeabschätzung (DPIA) in bestimmten Situationen durchgeführt werden muss. Sie schreibt Ihnen jedoch nicht vor, *wie* Sie diese tatsächlich durchzuführen haben. Dennoch spezifiziert die Verordnung einige Mindestanforderungen an die Datenschutzfolgeabschätzung (DPIA).

Welche Aktivität sollte angesichts dieser Mindestanforderungen **immer** Teil einer Datenschutzfolgeabschätzung (DPIA) sein?

A) Die Erarbeitung eines Verfahrens bezüglich des Auskunftsrechts betroffener Personen, um die Rechte der betroffenen Personen zu wahren
B) Die Identifizierung der verarbeiteten personenbezogenen Daten und der Zweck der Verarbeitung
C) Die Benachrichtigung der betroffenen Personen, dass eine Bewertung stattfinden wird und die Anforderung ihrer ausdrücklichen Einwilligung
D) Die Erarbeitung eines Notfallplans und die Festlegung angemessener Sicherheitsmassnahmen, um Verletzungen des Schutzes personenbezogener Daten zu vermeiden

29 / 40
Ein Unternehmen hat den Entschluss gefasst, seine Kundendaten besser zu nutzen, um Trends entdecken und analysieren und bessere Prognosen erstellen zu können. Dazu soll eine neue Unternehmenseinheit aufgebaut werden. Die Datenspezialisten werden mit Hilfe der neuesten Tools für die Datenanalyse ein Data Warehouse einführen.

Sie sind der Datenschutzbeauftragte (DSB) und haben ernsthafte Bedenken geäussert, da es sich hierbei um ein hoch riskantes Unterfangen handelt, dass sich negativ auf die Rechte der betroffenen Personen auswirken kann. Sowohl der CIO als auch der CEO wollen die Entwicklungen jedoch fortführen und scheinen nicht auf Ihre Bedenken reagieren zu wollen.

Wie gehen Sie in einem solchen Fall am **besten** vor?

A) Sie führen eine Datenschutzfolgeabschätzung (DPIA) durch und besprechen das Ergebnis und die möglichen Massnahmen zur Eindämmung des Risikos mit dem Vorstand und den anderen Stakeholdern.
B) Sie beteiligen den CIO an der Datenanonymisierung damit die DSGVO nicht mehr greift.
C) Sie richten eine Kundenumfrage ein, um sich direkt an die Kunden zu wenden und deren ausdrückliche Einwilligung für diese Verarbeitung ihrer personenbezogenen Daten einzuholen.
D) Sie wenden sich an die Aufsichtsbehörde, holen deren Meinung zu der geplanten Verarbeitung personenbezogener Daten ein und bitten die Behörde um Unterstützung bei der Erläuterung der Risiken.

30 / 40
Warum kann eine Datenschutzfolgeabschätzung (DPIA) als Teil des Risikomanagements einer Organisation betrachtet werden?

A) Eine Datenschutzfolgeabschätzung dient der Identifizierung von Risiken für betroffene Personen, die von der Organisation eingedämmt werden müssen.
B) Eine Datenschutzfolgeabschätzung dient der Identifizierung von Risiken für die Organisation, die von der Organisation eingedämmt werden müssen.
C) Eine Datenschutzfolgeabschätzung dient der Abschätzung der Folgen und dies ist für die Risikokategorisierung erforderlich.
D) Eine Organisation muss zur Konformität (Compliance) mit der DSGVO eine Datenschutzfolgeabschätzung durchführen.

31 / 40
Wichtig im Rahmen einer Datenschutzfolgeabschätzung (DPIA) ist die Bewertung der Risiken für den Datenschutz. Der nächste Schritt besteht darin, diese Risiken zu eliminieren oder auf ein annehmbares Mass (Risikoreaktion) zu reduzieren.

Bei welcher Massnahme handelt es sich um eine typische Risikoreaktion?

A) Die Festlegung von Kennzahlen zur Messung der Wirksamkeit
B) Die Reduzierung der Menge an erhobenen Daten
C) Die Einführung eines Datenschutzrisikoregisters
D) Die Freigabe und Aufzeichnung der Ergebnisse einer Datenschutzfolgeabschätzung (DPIA)

32 / 40
Muss eine Datenschutzfolgeabschätzung (DPIA) durchgeführt werden, so sind laut der DSGVO mehrere Grundsätze zu beachten Zwei dieser Grundsätze sind die Bewertung der Verhältnismässigkeit und der Notwendigkeit, sowie eine Bewertung der zur Bewältigung der identifizierten Risiken geplanten Abhilfemassnahmen.

Welches weitere Element muss laut DSGVO in einer Datenschutzfolgeabschätzung enthalten sein?

A) Ein Protokoll, wie im Falle von Verletzungen des Schutzes personenbezogener Daten zu verfahren ist
B) Ein öffentlicher Bericht über das Ergebnis der Datenschutzfolgeabschätzung
C) Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

33 / 40
Sie sind in Ihrer Organisation für ein Projekt verantwortlich, bei dem auch personenbezogene Daten verarbeitet werden. Im Rahmen Ihrer Verantwortung entscheiden Sie eine Datenschutzfolgeabschätzung (DPIA) durchzuführen und mit dem Datenmapping zu beginnen.

Warum ist das Datenmapping ein sinnvoller Bestandteil des DPIA-Verfahrens?

A) Durch das Datenmapping verschafft man sich einen Überblick über die Risiken für personenbezogene Daten
B) Durch das Datenmapping verschafft man sich einen Überblick über die bei der Verarbeitung personenbezogener Daten eingesetzten Systeme
C) Das Datenmapping trägt dazu bei, den Zweck der Datenverarbeitung zu identifizieren

34 / 40
Eine Organisation fällt bezüglich ihrer Kunden automatisierte Entscheidungen, die auf Profiling basieren.

Welcher Aspekt einer Datenschutzfolgeabschätzung (DPIA) ist in diesem Fall am **meisten** zu beachten?

A) Die Bewertung, ob für diese Verarbeitungstätigkeit eine Datenschutzfolgeabschätzung durchgeführt werden muss
B) Die Bewertung, wann die Daten gelöscht werden
C) Massnahmen zum Schutz der Rechte der betroffenen Personen durch das Ermöglichen menschlichen Eingreifens
D) Massnahmen, die der Sicherheit der Daten dienen und verhindern, dass die betroffenen Personen Zugriff auf diese erhalten

35 / 40
Sie sind in Ihrer Organisation für eine Datenschutzfolgeabschätzung (DPIA) verantwortlich. Im Zusammenhang mit dieser Datenschutzfolgeabschätzung konsultieren Sie eine Reihe von Kollegen, um eine ordnungsgemässe Beschreibung der für die Datenverarbeitung geplanten Tätigkeiten und Zwecke zu erstellen. Im Laufe dieser Konsultation zeigt sich, dass bei der Verarbeitung anscheinend personenbezogene Daten erhoben werden, die zwar für die aktuellen Zwecke nicht unbedingt erforderlich sind, sich für zukünftige Zwecke jedoch als nützlich erweisen könnten. Die Erhebung dieser Daten mit dem aktuellen Prozess zu verbinden ist effizienter.

Was sollten Sie in dieser Situation tun?

A) Sie sollten die Verarbeitung zulassen, weil Effizienz ein legitimes Interesse Ihrer Organisation entsprechend Artikel 6 der DSGVO darstellt.
B) Sie sollten fordern, dass die zusätzlichen Daten nicht mehr erhoben werden, da sie für den Zweck der Datenverarbeitung, für die die Datenschutzfolgeabschätzung durchgeführt wird, nicht erforderlich sind.
C) Sie sollten fordern, dass die Kollegen Ihnen einen legitimen Rechtsgrund für die Verarbeitung der zusätzlichen Daten entsprechend Artikel 6 der DSGVO bieten und die Verarbeitung zulassen.
D) Sie sollten fordern, dass die Daten entsprechend gesichert werden, um eine Verletzung des Schutzes personenbezogener Daten zu verhindern.

36 / 40
Sie führen für einen neuen Service Ihres Unternehmens, bei dem personenbezogene Daten der Kunden in grossem Umfang verarbeitet werden, eine Datenschutzfolgeabschätzung (DPIA) durch. F ür die Verarbeitung liegen berechtigte Gründe und ein festgelegter, eindeutiger Zweck vor. Ausserdem werden geeignete Massnahmen umgesetzt, um die Risiken für die Rechte der betroffenen Personen abzumildern. Es ist jedoch klar, dass der Service nur Erfolg haben wird, wenn er von den Kunden akzeptiert wird.

Welche spezifische Massnahme sollten Sie bezüglich des Verfahrens der Datenschutzfolgeabschätzung in diesem spezifischen Fall ergreifen?

A) Sie sollten sich an die Kunden oder deren Vertreter wenden und deren Meinung zur Verarbeitung ihrer personenbezogenen Daten einholen
B) Sie sollten sich an die Aufsichtsbehörde wenden und sich die Rechtmässigkeit der Verarbeitung bestätigen lassen
C) Sie sollten einen Helpdesk einrichten, an den sich Kunden wenden und sich den Service nach dem Rollout erklären lassen können
D) Sie sollten einen Bericht über die Datenschutzfolgeabschätzung an die Kunden senden, um diesen zu versichern, dass Massnahmen zur Abminderung des Risikos ergriffen wurden

37 / 40
Sie arbeiten als Datenschutzbeauftragter (DSB) in einem grossen Logistikunternehmen mit internationaler Kundschaft. Der Leiter der Personalabteilung berichtet, dass er einen verschlü sselten USB-Stick mit den Mitarbeiterdaten von 35 Mitarbeitern verlegt oder verloren hat.

Warum ist dies unter der DSGVO als Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden?

A) Ein Sicherheitsvorfall, der mit einem Verlust an vertraulichen Unternehmendaten einhergeht, ist als Verletzung des Schutzes personenbezogener Daten zu melden.
B) Der Vorfall ist zu melden, weil der Verlust eines Geräts mit personenbezogenen Daten ein Risiko für die Rechte und Freiheiten der natürlichen Personen darstellt.
C) Der Vorfall ist unverzüglich zu melden, damit die Aufsichtsbehörde die 35 Mitarbeiter über die Verletzung des Schutzes ihrer personenbezogenen Daten informieren kann.

38 / 40
Wann muss eine Organisation die Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde melden?

A) Immer dann, wenn ein Vorfall wahrscheinlich mit einem Risiko für die Rechte und Freiheiten der betroffenen Personen einhergeht
B) Immer dann, wenn eine Bedrohung der Sicherheit die Rechte und Freiheiten der betroffenen Personen gefährdet
C) Nur dann, wenn eine Organisation nicht in der Lage ist, den Vorfall innerhalb von 72 Stunden ab Eintreten zu lösen
D) Nur dann, wenn der Vorfall innerhalb von 72 Stunden ab Eintreten erkannt wird

39 / 40
Wann muss eine Organisation die Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen melden?

A) Immer dann, wenn eine Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem 'hohen Risiko' für die Rechte und Freiheiten der betroffenen Personen führt.
B) Immer dann, wenn ein Sicherheitsvorfall die Rechte und Freiheiten der betroffenen Personen gefährdet.
C) Nur wenn die Aufsichtsbehörde es als erforderlich erachtet, dass die betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten informiert werden.
D) Nur bei böswilliger Absicht, wenn personenbezogene Daten durch externe Akteure, wie zum Beispiel Cyberkriminelle gefährdet werden.

40 / 40
Jede Organisation wird immer wieder mit Verletzungen des Schutzes personenbezogener Daten zu tun haben, die an die Aufsichtsbehörde zu melden sind. Da der Meldeprozess immer wieder durchzuführen ist, empfiehlt es sich eine Meldevorlage anzufertigen, die folgende Punkte umfasst:

- die Art der Verletzung des Schutzes personenbezogener Daten
- die wahrscheinlichen Folgen
- die Massnahmen zur Eindämmung dieser Folgen

Welche weiteren Elementen sollten in der Vorlage enthalten sein?

A) - der Name und die Kontaktdaten des CEO
- der Notfallmanagementplan
B) - die Zahl der betroffenen Personen
- den Namen der Person, die für die Verletzung des Schutzes personenbezogener Daten verantwortlich ist.
C) - die Zahl der betroffenen Personen
- den Namen und die Kontaktdaten des Datenschutzbeauftragten und anderer Kontaktstellen
D) - die Nummer des Sicherheitsvorfalls
- die Analyse der Bedrohungen der Cybersicherheit

Antwortschlüssel

1 / 40
Welches Dokument muss der Verantwortliche betroffenen Personen zur Verfügung stellen?

A) Datenschutzpolitik
B) Richtlinie zur fairen Nutzung
C) Richtlinie zum Zugriffsmanagement
D) Richtlinie zur Informationssicherheit

A) Richtig. Laut der DSGVO müssen die Datenschutzrichtlinien für die betroffenen Personen zugänglich sein. (Literatur A, Kapitel 16, Abschnitt Using policies to demonstrate compliance. E-Buch Seite 155/164: “Your privacy policy should be readily accessible...”)
B) Falsch. Diese Dokumente müssen für die betroffenen Personen nicht zugänglich sein.
C) Falsch. Diese Dokumente müssen für die betroffenen Personen nicht zugänglich sein.
D) Falsch. Diese Dokumente müssen für die betroffenen Personen nicht zugänglich sein.

2 / 40
Was muss eine gute Datenschutzpolitik aus Unternehmenssicht leisten?

A) Sie sorgt für den nötigen Datenschutz im Einklang mit Produktivität.
B) Sie definiert Ansprechpartner und Zuständigkeiten.
C) Sie erklärt, wie mit Verstössen umzugehen ist.
D) Sie erklärt die Notwendigkeit einer Datenschutzpolitik.

A) Richtig. (Literatur A, Kapitel 16, Abschnitt: Using policies to demonstrate compliance. E-Buch Seite 156/164)
B) Falsch. Dies ist keine wesentliche Anforderung an eine gute Datenschutzpolitik
C) Falsch. Dies ist keine wesentliche Anforderung an eine gute Datenschutzpolitik
D) Falsch. Dies ist keine wesentliche Anforderung an eine gute Datenschutzpolitik

3 / 40
Warum ist laut DSGVO die Wahrung von Datenschutz und Privatsphäre durch datenschutzfreundliche Voreinstellungen ein Grundprinzip des Datenschutzes?

A) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass jeweils nur die personenbezogenen Daten verarbeitet werden, die für den festgelegten Zweck erforderlich sind.
B) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass personenbezogene Daten nur entsprechend der Datenschutzpolitik erhoben werden.
C) Datenschutzfreundliche Voreinstellungen sorgen dafür, dass die betroffenen Personen die standardmässige Datenschutzpolitik akzeptieren, bevor personenbezogene Daten verarbeitet werden.

A) Richtig. Literatur A, Kapitel 5, Abschnitt: Privacy by design and default. (E-Buch Seite 67/164): “The controller shall implement appropriate….”
B) Falsch. Datenschutzfreundliche Voreinstellungen beziehen sich nicht auf die Datenerhebung
C) Falsch. Datenschutzfreundliche Voreinstellungen beziehen sich nicht auf die Einwilligung.

4 / 40
Ein Unternehmen startet ein Projekt zur Erstellung eines neuen kostenlosen Services für Verbraucher.

Wann ist der **beste** Zeitpunkt, um die Themen Privatsphäre und Datenschutz anzusprechen?

A) Datenschutz muss in der Umsetzungsphase des Projekts besprochen und umgesetzt werden.
B) Privatsphäre und Datenschutz müssen ab dem Start des Projekts gefördert werden.
C) Bei allen Projekten mit personenbezogenen Daten ist vor Projektabschluss ein Datenschutzaudit durchzuführen.
D) Da dieses Projekt darauf abzielt, einen kostenlosen Service für Verbraucher zu schaffen, muss der Datenschutz auf einer aktuellen Datenschutzerklärung beruhen.

A) Falsch. In der Umsetzungsphase ist es zu spät. Die Wahrung von Privatsphäre und Datenschutz ist entsprechend dem „Datenschutz durch Technikgestaltung“ ab Projektstart zu berücksichtigen.
B) Richtig. Dies entspricht dem Konzept Datenschutz durch Technikgestaltung. (Literatur A, Kapitel 5, Abschnitt: Privacy by design and default).
C) Falsch. Bei Projektabschluss ist es zu spät. Die Wahrung von Privatsphäre und Datenschutz ist entsprechend dem „Datenschutz durch Technikgestaltung“ ab Projektstart zu berücksichtigen.
D) Falsch. Unabhängig von den Projektleistungen ist die Wahrung von Privatsphäre und Datenschutz entsprechend dem „Datenschutz durch Technikgestaltung“ ab Projektstart zu berücksichtigen.

5 / 40
Eine Organisation plant den Aufbau einer neuen Abteilung. Als Dienstleister soll diese betroffenen Personen die Möglichkeit bieten, ihre personenbezogenen Daten so zu speichern, dass die Datenü bertragbarkeit zwischen verschiedenen Verantwortlichen erleichtert wird. Der CEO der Organisation bittet sie um Ihren Rat.

Warum sollte ein Datenschutzmanagementsystem (DSMS) umgesetzt werden?

A) Ein DSMS trägt dazu bei wichtige Daten in ein System zu bringen.
B) Ein DSMS hilft bei der Erhebung der zu übertragenden Daten und beim Verfassung einer Sicherheitspolitik.
C) Ein DSMS verbessert das Datenmanagement und senkt die Risiken für Daten und Informationssysteme.
D) Ein DSMS ist laut DSGVO verpflichtend.

A) Falsch. Ein DSMS zielt nicht darauf ab, Daten für ein System zu erheben, sondern verbessert das Datenmanagement der Organisation und senkt die Risiken für Unternehmensdaten.
B) Falsch. Ziel eines DSMS ist nicht die Datenerhebung. Das Verfassen und Umsetzen einer Sicherheitspolitik ist lediglich ein Teil des DSMS. Das System umfasst ausserdem eine Methodik, eine Strategie und eine Reihe an Richtlinien, Verfahren sowie technischen und sonstigen Tools.
C) Richtig. Ein Datenschutzmanagementsystem (DSMS) sorgt für ein besseres Datenmanagement und senkt das Risiko, dass:
• Daten möglicherweise gehackt oder gestohlen werden beziehungsweise. verloren gehen
• das Sicherheitsbewusstsein der Mitarbeiter, die mit den Daten arbeiten, unzureichend ist
• Organisationen sich nicht an die Datenschutzvorschriften halten und keine Methoden, Strategien und diverse Richtlinien, Verfahren sowie technischen und sonstigen Tools entwickeln und dann mit sehr hohen Strafen rechnen müssen. (Literatur B, Abschnitt 2.1 Introduction to phase 1)
D) Falsch. Die DSGVO erfordert einen ordnungsgemässen Schutz der Daten durch entsprechende organisatorische und technische Massnahmen. Sie schreibt jedoch nicht vor, wie diese Massnahmen aussehen. Ein DSMS ist daher ebenfalls nicht vorgeschrieben.

6 / 40
Warum sollte in der Vorbereitung zur Einführung eines Datenschutzmanagementsystems (DSMS) Datenvoraudits und -bewertungen durchgeführt werden?

A) Sie identifizieren Risiken in den Bereichen Datenschutz und Privatsphäre, Risiken für Einzelpersonen und Konformität (Compliance) sowie weitere Risiken, die die Organisation betreffen.
B) Sie bieten einen klaren Überblick über den Datenfluss innerhalb und ausserhalb der Organisation und ermöglichen dem Aufsichtsgremium damit, diese Datenflüsse zu bewerten.
C) Sie analysieren die Bereitschaft und das Bewusstsein des Vorstands, der Geschäftsführung und der Mitarbeiter für Datenschutz und Privatsphäre.
D) Sie bieten eine Bestandsaufnahme, wo sich die verschiedenen Arten von Daten innerhalb der Organisation befinden und wer diese Daten innerhalb der Organisation besitzt.

A) Richtig. Datenaudits und -bewertungen, die in dieser Phase durchgeführt werden, identifizieren die Risiken für Konformität und Einzelpersonen sowie weitere damit verbundene Risiken. Das Ergebnis bietet einen ersten Einblick in das, was ein DSMS bieten sollte. (Literatur B, Abschnitt 2.2.1. Phase 1: Data Protection and Privacy Preparation, AP#4 Perform Initial Data Audits and Assessments.)
B) Falsch. Datenaudits und -bewertungen dienen nicht der Entwicklung und Umsetzung eines Systems zur Dokumentation und Pflege von Flussdiagrammen für die Darstellung der Datenflüsse innerhalb und ausserhalb der Organisation. Das Aufsichtsgremium prüft und bewertet diese Datenflüsse nicht. Das Aufsichtsgremium prüft und bewertet die möglichen Datenschutzfolgen und -risiken und sorgt für entsprechende Massnahmen, um diese Risiken zu reduzieren.
C) Falsch. Datenaudits und -bewertungen dienen nicht in erster Linie der Analyse der Bereitschaft und des Bewusstseins von Vorstand, Geschäftsführung und Mitarbeitern für Datenschutz und Privatsphäre. Sie sollen aus einer breiteren Perspektive Einblick in die relevanten Risiken bieten.
D) Falsch. Datenaudits und -bewertungen dienen nicht zur Bestandsaufnahme, wo sich die verschiedenen Arten von Daten innerhalb der Organisation befinden und wer diese Daten innerhalb der Organisation besitzt.

7 / 40
Sie sind der neue Konzerndatenschutzbeauftragte des Unternehmens ABC. Der CEO sorgt sich über den Mangel an ordnungsgemässen Kontrollen zum Schutz der Daten, die innerhalb des Unternehmens, aber auch zwischen dem Unternehmen und externen Parteien erhoben, genutzt und offengelegt werden. Sie empfehlen dem CEO die Umsetzung eines Datenschutzmanagementsystems (DSMS)

Warum spielt die Bestandsaufnahme der Datenflüsse in dieser Phase eine wesentliche Rolle?

A) Um zu ermitteln, wie die Mitarbeiter zu Fragen des Datenschutzes stehen.
B) Um sich einen klaren Überblick zu verschaffen, welche Risiken bezüglich Datenschutz und Wahrung der Privatsphäre reduziert werden müssen.
C) Um Situationen zu identifizieren, in denen Mitarbeiter ihre privaten Angelegenheiten mit offiziellen Unternehmensangelegenheiten vermischen.
D) Um das Bewusstsein der Mitarbeiter für Fragen des Datenschutzes und der Privatsphäre bei ihrer Arbeit zu stärken.

A) Falsch. Eine Bestandsaufnahme der Datenflüsse ermittelt nicht die Meinung der Mitarbeiter zu Fragen des Datenschutzes.
B) Richtig. Die Bestandsaufnahme zeigt, über welche Daten das Unternehmen verfügt und wo Risiken bez üglich des Zugriffs auf diese Daten, des Teilens und der Nutzung dieser Daten bestehen. So kann das Unternehmen einen Massnahmenplan aufstellen, um diese Risiken mit möglichst geringen Auswirkungen auf den Betrieb des Unternehmens zu reduzieren. (Literatur B, DPMS, Phase 1-Preparations, Products and outcome.)
C) Falsch. Eine Privatsphärenanalyse hat nichts mit den privaten Angelegenheiten der einzelnen Mitarbeiter zu tun.
D) Falsch. Dies kann zwar ein Nebeneffekt sein, wenn Mitarbeiter an der Erhebung von Informationen beteiligt sind, es ist aber nicht das Hauptziel. Dieser Punkt gehört eher in Phase 3, in der Schulungen zur Privatsphäre durchgeführt werden.

8 / 40
Was ist für die Umsetzung der organisatorischen Strukturen und Mechanismen erforderlich, die mit der Einführung der Phase 2 „Organisation von Datenschutz und Privatsphäre“ eines Datenschutzmanagementsystems (DSMS) einhergehen?

A) Die Auditierung der Massnahmen und Kontrollen im Bereich Privatsphäre und Datenschutz zur Identifizierung eventueller Lücken und Fehler.
B) Das Denken an Datenschutz und Privatsphäre muss im gesamten Unternehmen verankert werden, um Bewusstsein für Datenschutz und Privatsphäre zu schaffen.
C) Die Mitarbeiter müssen über den Stand des Datenschutz- und Privatsphärenprogramms informiert sein, um die Anforderungen des DSMS erfüllen zu können.
D) Regelmässige Meldungen an die obere Geschäftsführung, damit diese sich mit der Leistung des Datenschutzprogramms auseinandersetzt und diese fördert.

A) Falsch. Eine Auditierung kann erst nach vollständiger Implementierung erfolgen. Dies ist das Ergebnis der Phase 5.
B) Richtig. Das Bewusstsein für Datenschutz und Privatsphäre ist für die Schritte und Massnahmen, die zur Einhaltung der Anforderungen ergriffen werden müssen, von wesentlicher Bedeutung. Die Verbesserung von Datenschutz und Privatsphäre erfordert die kontinuierliche Überwachung der Datenverarbeitung. Dies sollte auf der Grundlage eines gut entwickelten Bewusstseins für Datenschutz und Privatsphäre aller Mitarbeiter und der oberen Geschäftsführung erfolgen. (Literatur B, Abschnitt 2.2.2., Step OS# 5 , siehe 5.2 Abschnitt e)
C) Falsch. Der Stand des Programms ist für die Mitarbeiter zwar wichtig, bedeutet jedoch nicht, dass die organisatorischen Strukturen und Mechanismen umgesetzt werden.
D) Falsch. Regelmässige Meldungen führen im Allgemeinen nicht direkt zur Einführung der erforderlichen organisatorischen Strukturen und Mechanismen und sollten nicht auf die obere Geschäftsführung beschränkt werden.

9 / 40
Das Datenschutzprogramm ist in der Datenschutzerklärung des Unternehmens verankert.

Welcher Aspekt ist hinsichtlich der Datenschutzerklärung **nicht** wichtig?

A) Die ordnungsgemässe und wirksame Anpassung an die Mission des Unternehmens
B) Die Erarbeitung der Aufgaben, Pflichten und Rollen der mit den Datenschutzpraktiken betrauten Personen
C) Die detaillierte Beschreibung der Strategien zur Wahrung von Datenschutz und Privatsphäre
D) Die Betonung, wie viel Wert das Unternehmen auf Datenschutz und Privatsphäre legt

A) Falsch. Die Anpassung der Datenschutzerklärung an die Mission des Unternehmens ist ein wichtiger Grundsatz, denn Datenschutz und Wahrung der Privatsphäre müssen in die Funktionen, Aktivitäten und Prozesse des Unternehmens eingebettet sein.
B) Richtig. Die Einzelheiten zu den Datenschutzpraktiken sind bei der Datenschutzerklärung nicht wichtig. Dieser Aspekt wird während der Umsetzung der Praktiken zu Datenschutz und Privatsphäre behandelt. (Literatur B, Abschnitt 2.2.2, Step OS#1, siehe 1.5 zusammen mit Step OS#2)
C) Falsch. Die detaillierte Beschreibung der Strategien zur Wahrung von Datenschutz und Privatsphäre ist wichtig, da es die allgemeine Richtung für den Datenschutz und die Wahrung der Privatsphäre im Unternehmen vorgibt.
D) Falsch. Es ist wichtig, zu betonen, wie viel Wert das Unternehmen auf Datenschutz und Privatsphäre legt, da dies zeigt, dass sich das Unternehmen zu Datenschutz und Wahrung der Privatsphäre verpflichtet fühlt.

10 / 40
Einer der entscheidendsten Faktoren für eine erfolgreiche Umsetzung des Datenschutzprogramms im Unternehmen ist die Unterstützung seitens der oberen Geschäftsführung.

Was ist **kein** Zeichen für die Unterstützung des Datenschutzprogramms seitens der oberen Geschäftsführung?

A) Die Information an die Mitarbeiter, wie wichtig Datenschutz und Privatsphäre sind
B) Die Übertragung der Verantwortung und Zuständigkeit für Initiativen im Bereich Datenschutz und Privatsphäre an den Datenschutzbeauftragten und die Prozessverantwortlichen
C) Die Bereitstellung finanzieller Mittel zur Unterstützung von Aktivitäten in den Bereichen Datenschutz und Privatsphäre

A) Falsch. Die Mitteilung der Wichtigkeit von Datenschutz und Privatsphäre an alle Manager und Mitarbeiter ist durchaus ein Zeichen für das Engagement und die Unterstützung seitens der oberen Geschäftsführung.
B) Richtig. Die Übertragung der Verantwortung für Datenschutz und die Wahrung der Privatsphäre an den Datenschutzbeauftragten (DSB) ist kein Zeichen für die Unterstützung seitens der oberen Geschäftsfü hrung. Die obere Geschäftsführung kann zwar Aufgaben delegieren, nicht aber die Verantwortung abgeben. (Literatur B, Abschnitt 2.2.2, Step OS#3, siehe 2.2)
C) Falsch. Die Bereitstellung angemessener finanzieller Mittel zur Unterstützung von Aktivitäten in den Bereichen Datenschutz und Privatsphäre zeigt, dass die obere Geschäftsführung keine leeren Versprechungen macht.

11 / 40
Im Rahmen eines Datenschutzprogramms hat es sich bewährt, ein Datenklassifikationssystem zu erstellen, um zu sehen, welches Mass an Schutz für personenbezogene Daten erforderlich ist.

Was ist der **primäre** Zweck eines Datenklassifikationssystems?

A) Die entsprechende Kennzeichnung der unterschiedlichen Datenkategorien zu ermöglichen
B) Die Umsetzung angemessener Kontrollen im Bereich Datenschutz und Privatsphäre für unterschiedliche Datenkategorien zu ermöglichen
C) Der Schutz aller verarbeiteten Daten sicherzustellen
D) Den Zugriff auf verschiedene Datenkategorien per Zielgruppe zu beschränken

A) Falsch. Die Kennzeichnung ist zwar erforderlich, um die verschiedenen Klassifikationsstufen der Daten anzuzeigen, aber dabei handelt es sich eher um eine Massnahme im Rahmen der Umsetzung und nicht um den primären Zweck.
B) Richtig. Dies ist die beste Antwort, denn das primäre Ziel des Datenklassifikationssystems ist es, die Umsetzung von Datenschutzkontrollen entsprechend der verschieden Stufen der Vertraulichkeit und Sensibilität der Daten umzusetzen. (Literatur B, Abschnitt 2.2.3, Step OS#3, siehe -2.2)
C) Falsch. Dieses Ziel ist zu weit und allgemein gefasst und unterscheidet nicht zwischen den verschiedenen Sicherheits- und Schutzniveaus.
D) Falsch. Nutzt man ein Datenklassifikationssystem zur Einschränkung des Zugriffs auf die diversen Datenkategorien, so erfolgt die Einschränkung des Zugriffs nicht für bestimmte Zielgruppen der Benutzer, sondern bezogen auf ihre Rollen und den Wissensbedarf.

12 / 40
Sie wurden als Datenschutzbeauftragter (DSB) eines globalen Unternehmens eingestellt. Eine ihrer ersten Aufgaben besteht darin, für das Unternehmen eine Reihe von Strategien, Plänen und Richtlinien für den Datenschutz und die Privatsphäre zu entwickeln und umzusetzen.

Was sollten Sie in Phase 3 „Entwicklung und Umsetzung von Datenschutz und Privatsphäre“ als **erstes** tun?

A) Sie sollten die Bedürfnisse und Anforderungen Ihres Unternehmens im Bereich Datenschutz analysieren und definieren.
B) Sie sollten das Wissen und Verstehen der Mitarbeiter hinsichtlich der Begriffe des Datenschutzes und der Privatsphäre einschätzen.
C) Sie sollten die Best Practices der Branche recherchieren und auf Ihr Unternehmen anpassen.
D) Sie sollten die allgemeine Datenschutz- und Privatsphärenlandschaft verstehen.

A) Richtig. Als erstes müssen Sie die Bedürfnisse und Anforderungen Ihres Unternehmens kennen und festlegen, um die Ziele und Zielsetzungen für Strategien, Pläne und Richtlinien in den Bereichen Datenschutz und Privatsphäre festlegen zu können. (Literatur B, Abschnitt 2.2.3, Schritt DI#1)
B) Falsch. Das können Sie erst machen, nachdem Sie die Bedürfnisse und Anforderungen Ihres Unternehmens analysiert und festgelegt haben.
C) Falsch. Sie können die Best Practices der Branche erst an Ihr Unternehmen anpassen, nachdem Sie die Bedürfnisse und Anforderungen Ihres Unternehmens analysiert und festgelegt haben.
D) Falsch. Was wirklich relevant ist können Sie erst wissen, nachdem Sie die Bedürfnisse und Anforderungen Ihres Unternehmens analysiert und festgelegt haben.

13 / 40
Eine der wichtigsten Anforderungen der DSGVO ist, dass ein Unternehmen Konformität (Compliance) nachweisen muss.

Welche Phase des Datenschutzmanagementsystems (DSMS) ist aus dieser Perspektive betrachtet am **wichtigsten**?

A) Phase 1, in der die Organisation auf den Datenschutz vorbereitet wird
B) Phase 2, in der die für den Datenschutz erforderlichen organisatorischen Strukturen und Mechanismen eingeführt werden
C) Phase 3, in der Datenschutzmassnahmen der Organisation entwickelt und umgesetzt werden
D) Phase 4, in der die Governance-Mechanismen für den Datenschutz der Organisation eingeführt werden

A) Falsch. Diese Phase bereitet die Organisation zwar auf die Umsetzung vor, umfasst jedoch noch keine wie auch immer geartete Form der Konformität. Konkrete Ziele in dieser Phase sind die Analyse der Anforderungen und Bedürfnisse bezüglich Datenschutz und Privatsphäre, die sich auf Ihr Unternehmen auswirken; die Sammlung der massgeblichen Gesetze, Normen und Vorschriften im Bereich Datenschutz und Privatsphäre sowie die Erstellung eines Massnahmenplans mit den erforderlichen Ressourcen, damit Sie Ihr Unternehmen darauf vorbereiten, dass es seine personenbezogenen Daten, Aktivitäten, Transaktionen und Geschäftstätigkeiten besser verwaltet und dabei die bestehenden Regeln und Vorschriften zu Datenschutz und Privatsphäre vollständig berü cksichtigt.
B) Falsch. Dies ist zwar wichtig, um eine Grundlage für die Umsetzung der Datenschutzanforderungen zu schaffen, nicht aber für die Konformität selbst. Konkrete Ziele in dieser Phase sind die Entwicklung und Einrichtung eines Datenschutzprogramms, Bestellung eines Datenschutzbeauftragten und die Verpflichtung aller im Datenschutz involvierten Parteien.
C) Richtig. Die Umsetzung von Verfahren, Richtlinien und Kontrollen ist ein Nachweis für Konformität. Konkrete Ziele in dieser Phase sind der Entwurf eines Datenklassifikationssystems sowie die Entwicklung und Umsetzung der Richtlinien, Verfahren und Kontrollen, die für die Umsetzung der Datenschutzgesetze und -anforderungen in Ihrem Unternehmen beziehungsweise Ihrer Organisation erforderlich sind (zum Beispiel zur Verwaltung sensibler Daten, der Ausführung des Trainingsplans, der Integration von Datenschutz in Ihre Geschäftstätigkeit etcetera), (Literatur B, Abschnitt 2.2.3, Einfü hrung Goal and objectives, und Schritt #DI 5 Execute DPP Integration Activities, und Phase 3 Implementation und outcomes sowie Literatur C DSGVO Art. 24(1)).
D) Falsch. Dies ist zwar für die langfristige Konformität wichtig, muss aber zuerst umgesetzt werden. Konkrete Ziele in dieser Phase sind die Entwicklung und Einführung der Datenschutz-Governance-Strukturen (zum Beispiel ein Datenschutzprogramm, ein Datenschutzbeauftragter und häufig auch ein Datenschutzausschuss etceteraetera); die Verpflichtung aller in den Datenschutz involvierter Parteien; und die kontinuierliche Meldung aller Datenschutzprobleme in Ihrem Unternehmen beziehungsweise in Ihrer Organisation.

14 / 40
Sie sind Datenschutzbeauftragter und werden gebeten, zur Datenschutz-Governance beizutragen. Sie entscheiden, dass Ihr Unternehmen betroffenen Personen Datenschutzhinweise bereitstellen sollte, die die betroffenen Personen darüber informieren, wie ihre Daten verarbeitet werden und welche Kontrollen existieren.

Was sollten diese Datenschutzhinweise **nicht** enthalten?

A) Wie die Daten erhoben, genutzt, gepflegt, aufbewahrt und offenbart werden
B) Welche personenbezogenen Daten erhoben werden
C) Welche Sicherheitsrichtlinien die Organisation umsetzt
D) Welche konkreten Kontrollen die betroffenen Personen nutzen können

A) Falsch. Dies ist Teil der Datenschutzhinweise für betroffene Personen in Schritt GR #2, Abschnitt 2.2.4.
B) Falsch. Dies ist Teil der Datenschutzhinweise für betroffene Personen in Schritt GR #2, Abschnitt 2.2.4.
C) Richtig. Datenschutzhinweise enthalten keine Informationen darüber, welche Sicherheitsrichtlinien die Organisation umsetzt. Würde die Organisation ihre Sicherheitsrichtlinien gegenüber einzelnen Personen bekanntgeben, so würde das Risiko eines Hackerangriffs wachsen. Dies ist nicht im Interesse der betroffenen Personen, die ihre personenbezogenen Daten schützen möchten. Eine Datenschutzerklärung sollte nur das Recht der betroffenen Person auf Auskunft darüber abdecken, wie ihre personenbezogenen Daten erhoben und verarbeitet werden und welche Kontrollen diesbezü glich existieren. (Literatur B, Abschnitt 2.2.4., Schritt GR # 2, siehe 2.2.4)
D) Falsch. Dies ist Teil der Datenschutzhinweise für betroffene Personen in Schritt GR #2, Abschnitt 2.2.4.

15 / 40
Sie sind Datenschutzbeauftragter (DSB) in einem Beratungsunternehmen und müssen ein Incident Management System umsetzen.

Was würde ein solches System beinhalten?

A) Die Erfassung aller verarbeiteten Daten und deren Aufbewahrung an einem sicheren Ort, damit sie im Falle eines Incidents (Vorfalls) abgerufen und die zu ergreifenden Massnahmen auf ein Minimum reduziert werden können
B) Das Erkennen von Incidents, die Reaktion auf unmittelbare und langfristige Belange, die Verfolgung der Vorfälle, um die Wirksamkeit der ergriffenen Massnahmen sicherzustellen
C) Die Registrierung aller Incidents (und die Durchführung einer Datenschutzfolgeabschätzung zur Analyse der Risiken und Aufstellung eines Verbesserungsplans
D) Die Registrierung aller Incidents und ihre Meldung an das Aufsichtsgremium zur Bewertung der Datenflüsse und Verbesserung der vom Aufsichtsgremium geforderten Sicherheitspolitik

A) Falsch. Die Erfassung und Aufbewahrung der Daten ist nur ein Teil der Datenspeicherung. Die Erstellung von Backups hat nichts mit dem Management der Incidents selbst zu tun und führt nicht zu einer Verbesserung im Umgang damit.
B) Richtig. Dies beschreibt den Zyklus des Incident Managements. (Literatur A, Kapitel 14, S. 241 (E-Buch 135))
C) Falsch. Das Incident Management selbst enthält keine Datenschutzfolgeabschätzung (DPIA). Eine Datenschutzfolgeabschätzung ist nur wichtig, wenn beispielsweise ein vollständig oder teilweise neues System beziehungsweise eine vollständig oder teilweise neue Anwendung oder Software zur Verarbeitung der Daten eingesetzt wird.
D) Falsch. Incidents sind an die verantwortlichen Mitarbeiter zu melden. Das Aufsichtsgremium prüft und bewertet diese Datenflüsse nicht. Das Aufsichtsgremium prüft und bewertet die möglichen Datenschutzfolgen und -risiken und sorgt für entsprechende Massnahmen, um diese Risiken zu reduzieren.

16 / 40

Ein Gesundheitsinstitut arbeitet eng mit zwei anderen Gesundheitsinstituten zusammen, um eine mobile Anwendung zur Patientenüberwachung zu entwickeln. Die Institute entscheiden sich, die Ergebnisse der neuen mobilen Anwendung mit Hilfe einer Pilotanwendung zu prüfen. Bei dieser Pilotanwendung geben Ärzte und Patienten ihre personenbezogenen Daten und Qualifikationen sowie medizinische Daten in die mobile Anwendung ein. Im Rahmen des Pilotverfahrens wird eine Sicherheitsprüfung durchgeführt. Die Testergebnisse zeigen, dass die mobile Anwendung alles andere als sicher ist. Sie kann leicht gehackt und Patientendaten dann geändert werden. Ausserdem ist es möglich, dass Hacker die Rolle des Arztes übernehmen und die medizinischen Daten der Patienten ändern.

Was sollte der von den drei Gesundheitsinstituten ernannte Datenschutzbeauftragte (DSB) im Interesse der betroffenen Personen tun?

A) Der DSB muss nichts tun, da es sich nur um eine Pilotanwendung handelt, an der nur ein relativ kleiner Teil der Patientenpopulation teilnimmt.

B) Der DSB muss nichts tun, da es sich lediglich um eine Pilotanwendung handelt und daher kein hohes Risiko besteht, dass die Auswirkungen der entdeckten Schwachstellen tatsächlichen eintreten.

C) Der DSB muss die beteiligten Patienten und Ärzte informieren, da das Testergebnis für diese wahrscheinlich ein hohes Risiko beinhaltet. Darüber hinaus meldet er das Ergebnis auch an die Aufsichtsbehörde.

D) Der DSB nutzt den Testbericht, um die Sicherheitsrisiken an die für die mobile Anwendung erforderlichen Sicherheitsstandards anzupassen und informiert die Überwachungsbehörde.

A) Falsch. Die Zahl der Patienten ist nicht der ausschlaggebende Faktor für eine mögliche Verletzung des Schutzes der personenbezogenen Daten der Patienten. Ausschlaggebender Faktor ist die Einschätzung, dass eine Eintrittswahrscheinlichkeit für ein hohes Risiko besteht.

B) Falsch. Die Tatsache, dass es sich hier um eine Pilotanwendung handelt, ist kein Grund, Patienten einem hohen Risiko auszusetzen, für das eine Eintrittswahrscheinlichkeit besteht. Dies hat keine Relevanz für die Art und Weise, in der die mobile Anwendung umgesetzt wird.

C) Richtig. Der Test zeigt keine Anzeichen für eine Verschlüsselung, da Hacker sich einfach Zugriff zu der mobilen Anwendung verschaffen und Daten ändern können. Der Verantwortliche hat nur unzureichende Massnahmen getroffen, um sicherzustellen, dass kein hohes Risiko eintreten wird. (Literatur A, Kapitel 14, Abschnitt Notification. E-Buch, Seiten 135, 136)

D) Falsch. Dies kann zwar zur Reduzierung/Eindämmung des künftigen Risikos beitragen, aber das Risiko für Patienten und Ärzte bleibt hoch, daher sollten diese über die Situation informiert werden.

17 / 40
Was ist das **wichtigste** Argument für Sie, eine externe Partei mit der Durchführung von Datenschutzbewertungen zu betrauen?

A) Um zu sehen, ob Ihre Datenschutzaktivitäten den in der Branche üblichen Standards entsprechen
B) Um eine unabhängige Validierung Ihrer Konformität (Compliance) mit den internen Datenschutzrichtlinien und geltenden rechtlichen Anforderungen zu erhalten
C) Um die Glaubwürdigkeit Ihres Datenschutzprogramms zu verbessern
D) Um Zeitdruck und Budgetzwängen zu begegnen, die in Ihrem Datenschutzprogramm eine wichtige Rolle spielen

A) Falsch. Der Grund, warum eine externe Partei mit der Bewertung des Datenschutzes betraut wird, ist die Validierung der Konformität mit den internen Datenschutzrichtlinien und den geltenden rechtlichen Anforderungen.
B) Richtig. Das Unternehmen beziehungsweise die Organisation kann die Durchführung einer Bewertung durch einen externen Dienstleister fordern, um die Konformität mit den internen Datenschutzrichtlinien und den geltenden rechtlichen Anforderungen zu validieren. Eine unabhängige externe Partei kann dabei dem Unternehmen eine neutrale Sichtweise auf die Durchführung des Datenschutzes und der Wahrung der Privatsphäre bieten. Grund hierfür ist, dass die externe Partei nicht mit den Systemen und Prozessen des Unternehmens befasst ist und Dinge daher neutral und unvoreingenommen betrachten kann. (Literatur B, Kapitel 2.2 Phase 5 Schritt RI#2)
C) Falsch. Eine Verbesserung der Glaubwürdigkeit des Datenschutzprogramms ist kein Grund für die Verpflichtung einer externen Partei. Ihr Datenschutzprogramm wird erst dann glaubwürdig sein, wenn Sie alle Phasen eines vollständig integrierten Datenschutzmanagementsystems (DSBS) umgesetzt haben.
D) Falsch. Bei Zeitdruck und Budgetzwängen verlassen sich Organisationen in der Regel bei der Durchfü hrung von Datenschutzbewertungen auf interne Mitarbeiter.

18 / 40
In einem Unternehmen kam es gerade zu einer Verletzung des Schutzes personenbezogener Daten, die das Customer Relationship Management (CRM) System über zwei Stunden lahmgelegt hat. Als Datenschutzbeauftragter (DSB) des Unternehmens entschliessen Sie sich unter anderem eine ad hoc Datenschutzbewertung durchzuführen.

Was ist eines der **wichtigsten** Ziele einer solchen unangekündigten Bewertung?

A) Beratung für eine entsprechende Benachrichtigung der Kunden zu geben
B) Bewertung des Ausmasses des Schadens, der durch die Verletzung des Schutzes personenbezogener Daten verursacht wurde
C) Ermittlung der Risiken für den Datenschutz
D) Identifizierung der für die Verletzung des Schutzes personenbezogener Daten verantwortlichen Personen

A) Falsch. Ratschläge für eine entsprechende Benachrichtigung der Kunden erfolgen im Rahmen der Untersuchung der Verletzung des Schutzes der personenbezogenen Daten und nicht im Rahmen einer ad hoc Bewertung.
B) Falsch. Die Bewertung des Schadensausmasses erfolgt im Rahmen der Untersuchung der Verletzung des Schutzes der personenbezogenen Daten und nicht im Rahmen einer ad hoc Bewertung.
C) Richtig. Eines der Ziele für die Durchführung einer ad hoc Bewertung nach Verletzung des Schutzes personenbezogener Daten ist die Ermittlung der Datenschutzrisiken, um sicherzustellen, dass eine ähnliche Verletzung des Schutzes personenbezogener Daten künftig nicht mehr auftreten wird. (Literatur B, Abschnitt 2.2.5, Schritt RI#3)
D) Falsch. Die Identifizierung der für die Verletzung des Schutzes personenbezogener Daten verantwortlichen Personen erfolgt im Rahmen der Untersuchung der Verletzung des Schutzes der personenbezogenen Daten und nicht im Rahmen einer ad hoc Bewertung.

19 / 40
Ein Unternehmen, das gleichzeitig Verantwortlicher für die Datenverarbeitung ist, kämpft seit einiger Zeit mit finanziellen Schwierigkeiten. Der Vorstand beschliesst, die Software des Datenschutzmanagementsystems (DSMS) nicht zu aktualisieren. Stattdessen bittet das Unternehmen die Aufsichtsbehörde, die Anwendung einer Datenschutzzertifizierung zu genehmigen. Dies spart dem Unternehmen viel Geld und bringt ihm wirtschaftlichen Mehrwert.

Sie sind der Datenschutzbeauftragte (DSB) dieses Verantwortlichen, welchen Rat sollten Sie dem Vorstand geben?

A) Das Verfahren zu verfolgen und die Datenschutzzertifizierung zu erwerben. Mit dem Zertifikat kann das Unternehmen nachweisen, dass es seine Pflichten als Verantwortlicher erfüllt.
B) Die Durchführung einer externen Datenschutzbewertung. Durch diese Massnahme wird zwar das gesamte Budget erschöpft, es wird aber auch sichergestellt, dass die technischen und organisatorischen Massnahmen ergriffen werden, die der Art, dem Umfang und dem Kontext der personenbezogenen Daten entsprechen.
C) Die Software des DSMS nur zu einem Drittel zu aktualisieren, wobei nur jene Teile aktualisiert werden, die laut einer internen Bewertung die meisten Sicherheitslücken aufweisen und aktualisiert werden mü ssen.
D) Das DSMS zu aktualisieren. Die Nichtaktualisierung des DSMS führt zu einem potenziellen Risiko der Nichtkonformität. Dies kann als Nichtdurchführung geeigneter technischer und organisatorischer Massnahmen seitens des Verantwortlichen gewertet werden.

A) Richtig. Der Zertifizierungsmechanismus kann seitens des Verantwortlichen als Nachweis der Konformität (Compliance) genutzt werden. (Literatur A, Kapitel 12 Demonstrating Compliance. Literatur C, Artikel 24 (3) DSGVO)
B) Falsch. Dies ist verglichen mit der Alternative einer von der Aufsichtsbehörde zugelassenen Datenschutzzertifizierung die schwächere Alternative und kann daher nicht als „geeignete “ Massnahme bezeichnet werden.
C) Falsch. Dies ist verglichen mit der Alternative einer von der Aufsichtsbehörde zugelassenen Datenschutzzertifizierung die schwächere Alternative und kann daher nicht als „geeignete “ Massnahme bezeichnet werden.
D) Falsch. Die Nichtdurchführung der Aktualisierung stellt an sich noch keine Nichtkonformität dar. Die Verantwortlichkeiten des Verantwortlichen basieren auf der Ergreifung „geeigneter“ Massnahmen, dies zeigt, dass auch andere Optionen möglich sind.

20 / 40
Ein beliebter Fitness-Club im Zentrum von Paris speichert seine Daten bei einem ebenfalls in Paris ansässigen Hosting-Unternehmen. Die Server, auf denen die Daten der Mitglieder des Fitnessclubs gespeichert sind, wurden vor kurzem von einem IT-Serviceunternehmen im Rahmen der regulären Instandhaltung überprüft. Am Tag nach dem Besuch des IT-Serviceunternehmens fällt der Server aus und verursacht einen Brand im Serverraum. Die Daten des Fitness-Clubs und deren Backups, die auf dem gleichen Server gespeichert waren, gehen bei dem Brand verloren. Eine Untersuchung ergibt, dass das Kühlsystem im Serverraum nicht gut funktionierte und das Überhitzen des Serversystems verursacht hat. Dem Instandhaltungstechniker war aufgefallen, dass die Temperatur im Raum ein wenig hoch war. Er hat dies aber nicht an das Serverunternehmen gemeldet, da er in Eile war und diesen Umstand nicht besonders aussergewöhnlich fand. Das Kühlsystem wird von dem Hostingunternehmen selbst gewartet.

Welche Partei ist am **wahrscheinlichsten** für den Vorfall verantwortlich?

A) Der Fitness-Club, weil die Organisation für die verlorenen Daten verantwortlich ist
B) Der Fitness-Club, weil er nicht angeordnet hat, dass die Backups auf einem anderen Server gespeichert werden müssen
C) Das Hostingunternehmen, weil dieses für die Sicherheit rund um die personenbezogenen Daten verantwortlich ist
D) Das IT-Unternehmen, da der Instandhaltungstechniker hätte melden müssen, dass die Temperatur im Serverraum ziemlich hoch ist

A) Falsch. Der Fitness-Club als Verantwortlicher muss nicht jedes Element der Auftragsverarbeitung der Daten festlegen. Die Sicherheit rund um die personenbezogenen Daten fällt unter die Verantwortung des Hostingunternehmens, des Auftragsverarbeiters selbst.
B) Falsch. Die Anweisung, wie Backups zu speichern sind fällt unter die Verantwortung des Hosting-Unternehmens, des Auftragsverarbeiters. Der Fitness-Club als Verantwortlicher muss nicht jedes Element der Auftragsverarbeitung der Daten festlegen.
C) Richtig. Das Hostingunternehmen ist als Auftragsverarbeiter für die Sicherheit rund um die personenbezogenen Daten verantwortlich. Der Fitness-Club als Verantwortlicher muss nicht jedes Element der Auftragsverarbeitung der Daten festlegen. (Literatur A, Kapitel 12, Abschnitt Data processors)
D) Falsch. Das IT-Unternehmen ist nicht dafür verantwortlich eine erhöhte Temperatur zu melden. Eine höhere Temperatur kann durch viele Faktoren verursacht werden. Die hohe Temperatur wurde nicht durch den Server selbst verursacht und fällt damit nicht unter die Verantwortung des IT-Unternehmens.

21 / 40
Ein Krankenhaus hat das Ausdrucken seiner Patientenrechnungen an eine Druckerei ausgelagert. Die Druckerei druckt auch Rechnungen für andere Unternehmen. Aufgrund einer Verwechslung von Namen und Adressen beim Sortieren in der Druckerei wurden einige Rechnungen an die falschen Patienten geschickt. Das Krankenhaus hatte seine Geschäfte sorgfältig analysiert. Das Krankenhaus verfügte über einen sehr robusten Verifizierungsprozess und vertragliche Vereinbarungen mit den Druckereien.

Warum ist die Druckerei wahrscheinlich haftbar?

A) Weil sie den Zweck der Auftragsverarbeitung bestimmt.
B) Weil sie die Druckverfahren bestimmt.
C) Weil sie bestimmt, welche Daten verarbeitet werden.
D) Weil sie auch Abrechnungen für andere Organisationen druckt.

Erläuterung auf der nächsten Seite.

A) Falsch. Die Verantwortung liegt laut DSGVO sowohl beim Verantwortlichen als auch beim Auftragsverarbeiter. Das Krankenhaus als Verantwortlicher legt den Zweck der Auftragsverarbeitung fest. Die Druckerei ist der Auftragsverarbeiter. Laut DSGVO liegt die Verantwortung für die Konformität (Compliance) mit den Prinzipien des Datenschutzes beim Verantwortlichen. Dieser muss auch den Konformitätsnachweis erbringen. Der Verantwortliche kann jedoch von der Haftung befreit werden, wenn er nachweisen kann, dass er in keiner Weise für den Schaden verantwortlich ist. Der Auftragsverarbeiter ist dann haftbar, wenn er ausserhalb oder entgegen der rechtmässigen Anweisungen des Verantwortlichen handelt. In dem hier vorliegenden Fall hat das Krankenhaus Massnahmen ergriffen, um die Konformität der Auftragsverarbeitung sicherzustellen. Damit liegt die Haftung wahrscheinlich bei der Druckerei.

B) Richtig. Die Verantwortung liegt laut DSGVO sowohl beim Verantwortlichen als auch beim Auftragsverarbeiter. Das Krankenhaus als Verantwortlicher legt den Zweck der Auftragsbearbeitung fest. Die Druckerei ist der Auftragsverarbeiter. Laut DSGVO liegt die Verantwortung für die Konformität (mit den Prinzipien des Datenschutzes beim Verantwortlichen. Dieser muss auch den Konformitätsnachweis erbringen. Der Verantwortliche kann jedoch von der Haftung befreit werden, wenn er nachweisen kann, dass er in keiner Weise für den Schaden verantwortlich ist. Der Auftragsverarbeiter ist dann haftbar, wenn er ausserhalb oder entgegen der rechtmässigen Anweisungen des Verantwortlichen handelt. In dem hier vorliegenden Fall hat das Krankenhaus Massnahmen ergriffen, um die Konformität der Auftragsverarbeitung sicherzustellen. Damit liegt die Haftung wahrscheinlich bei der Druckerei, da sie die Druckverfahren festlegt, die letztendlich dazu gef ührt haben, dass die Rechnungen an die falschen Patienten geschickt wurden. (Literatur A, Kapitel 12, Seiten 211-215)

C) Falsch. Die Verantwortung liegt laut DSGVO sowohl beim Verantwortlichen als auch beim Auftragsverarbeiter. Das Krankenhaus als Verantwortlicher legt den Zweck der Auftragsverarbeitung fest. Die Druckerei ist der Auftragsverarbeiter. Laut DSGVO liegt die Verantwortung für die Konformität mit den Prinzipien des Datenschutzes beim Verantwortlichen. Dieser muss auch den Konformitätsnachweis erbringen. Der Verantwortliche kann jedoch von der Haftung befreit werden, wenn er nachweisen kann, dass er in keiner Weise für den Schaden verantwortlich ist. Der Auftragsverarbeiter ist dann haftbar, wenn er ausserhalb oder entgegen der rechtmässigen Anweisungen des Verantwortlichen handelt. In dem hier vorliegenden Fall hat das Krankenhaus Massnahmen ergriffen, um die Konformität der Auftragsverarbeitung sicherzustellen. Damit liegt die Haftung wahrscheinlich bei der Druckerei.

D) Falsch. Die Verantwortung liegt laut DSGVO sowohl beim Verantwortlichen als auch beim Auftragsverarbeiter. Das Krankenhaus als Verantwortlicher legt den Zweck der Auftragsverarbeitung fest. Die Druckerei ist der Auftragsverarbeiter. Laut DSGVO liegt die Verantwortung für die Konformität mit den Prinzipien des Datenschutzes beim Verantwortlichen. Dieser muss auch den Konformitätsnachweis erbringen. Der Verantwortliche kann jedoch von der Haftung befreit werden, wenn er nachweisen kann, dass er in keiner Weise für den Schaden verantwortlich ist. Der Auftragsverarbeiter ist dann haftbar, wenn er ausserhalb oder entgegen der rechtmässigen Anweisungen des Verantwortlichen handelt. In dem hier vorliegenden Fall hat das Krankenhaus Massnahmen ergriffen, um die Konformität der Auftragsverarbeitung sicherzustellen. Damit liegt die Haftung wahrscheinlich bei der Druckerei.

22 / 40
Ein inhabergeführtes Haushaltwarengeschäft entschliesst sich, ein Website-Analyse-Unternehmen mit gezielter Werbung und Marketing zu beauftragen. Der Arzt und der Rechtsanwalt im gleichen Ort entschliessen sich ebenfalls, das gleiche Website-Analyse-Unternehmen zu beauftragen, das daneben noch andere Kunden hat.

Welche Organisation(en) müssen einen Datenschutzbeauftragten (DSB) bestellen?

A) Das inhabergeführte Haushaltswarengeschäft
B) Das inhabergeführte Haushaltswarengeschäft und das Website-Analyse-Unternehmen
C) Der Arzt und der Rechtsanwalt
D) Das Website-Analyse-Unternehmen

A) Falsch. Das Website-Analyse-Unternehmen muss einen Datenschutzbeauftragten bestellen. Sein Kerngeschäft besteht in der kontinuierlichen Verarbeitung und Analyse von personenbezogenen Daten im Auftrag seiner Kunden und das Unternehmen führt diese Tätigkeiten in grossem Umfang durch. Das kleine inhabergeführte Haushaltswarengeschäft, der Arzt und der Rechtsanwalt, verarbeiten zwar die personenbezogenen Daten ihrer Kunden, tun dies aber nicht in grossem Umfang.
B) Falsch. Das Website-Analyse-Unternehmen muss einen Datenschutzbeauftragten bestellen. Sein Kerngeschäft besteht in der kontinuierlichen Verarbeitung und Analyse von personenbezogenen Daten im Auftrag seiner Kunden und das Unternehmen führt diese Tätigkeiten in grossem Umfang durch. Das kleine inhabergeführte Haushaltswarengeschäft, der Arzt und der Rechtsanwalt, verarbeiten zwar die personenbezogenen Daten ihrer Kunden, tun dies aber nicht in grossem Umfang.
C) Falsch. Das Website-Analyse-Unternehmen muss einen Datenschutzbeauftragten bestellen. Sein Kerngeschäft besteht in der kontinuierlichen Verarbeitung und Analyse von personenbezogenen Daten im Auftrag seiner Kunden und das Unternehmen führt diese Tätigkeiten in grossem Umfang durch. Das kleine inhabergeführte Haushaltswarengeschäft, der Arzt und der Rechtsanwalt, verarbeiten zwar die personenbezogenen Daten ihrer Kunden, tun dies aber nicht in grossem Umfang.
D) Richtig. Das Website-Analyse-Unternehmen muss einen Datenschutzbeauftragten bestellen. Sein Kerngeschäft besteht in der kontinuierlichen Verarbeitung und Analyse von personenbezogenen Daten im Auftrag seiner Kunden und das Unternehmen führt diese Tätigkeiten in grossem Umfang durch. Das kleine inhabergeführte Haushaltswarengeschäft, der Arzt und der Rechtsanwalt, verarbeiten zwar die personenbezogenen Daten ihrer Kunden, tun dies aber nicht in grossem Umfang. (Literatur A, Kapitel 2 Einleitung und Literatur C Artikel 37 b DSGVO)

23 / 40
Auf der Insel Texel, einer kleinen Insel in der Nordsee, die zu den Niederlanden gehört, lebt ein Hausarzt. Er führt ein privates, gewinnorientiertes Unternehmen. Seine Arztpraxis hat 60 registrierte Patienten.

Welche Aussage bezüglich der Bestellung eines Datenschutzbeauftragten (DSB) ist korrekt?

A) Die Arztpraxis ist zu klein und gilt daher nicht als Praxis, die in grossem Umfang für medizinischen Daten verantwortlich ist beziehungsweise diese verarbeitet. Daher muss der Hausarzt keinen DSB bestellen.
B) Die Arztpraxis überwacht regelmässig und systematisch Patienten. Deshalb muss der Arzt einen DSB bestellen.
C) Der Hausarzt betreibt die einzige Arztpraxis auf der Insel. Er übt hinsichtlich seiner Patienten eine unabhängige und professionelle Rolle aus. Er kann Arzt und DSB in Personalunion sein.

A) Richtig. Die Verpflichtung zur Bestellung eines DSB gilt nur für Behörden, Stellen oder Unternehmen, deren Kerngeschäft aufgrund ihrer Art, ihres Geltungsbereichs oder der von ihnen verfolgten Zwecke in der umfangreichen Verarbeitung personenbezogener Daten beziehungsweise in der Verarbeitung besonderer Datenkategorien besteht oder deren Kerngeschäft es ist, in grossem Umfang besondere Kategorien personenbezogener Daten gemäss Artikel 9 und 10 der DSGVO zu verarbeiten. (Literatur C Artikel 9 und 10 DSGVO und Artikel 37 (1) b und c DSGVO; Literatur A, Kapitel 2, Einleitung)
B) Falsch. Die Patienten werden nicht systematisch überwacht, da sie den Hausarzt nur bei Bedarf aufsuchen. Auch medizinische Fragen beziehungsweise Gesundheitsprobleme werden nicht in grossem Umfang aufgezeichnet. Siehe Artikel 37 DSGVO.
C) Falsch. Der Hausarzt ist für die Verwaltung der Gesundheitsdaten seiner Patienten verantwortlich und führt seine Praxis als Unternehmen. Als Geschäftsführer seines Unternehmens hat er bezüglich der persönlichen Gesundheitsdaten seiner Patienten keine unabhängige Rolle und kann daher die Funktion des DSB nicht in Personalunion ausüben.

24 / 40
Laut der Datenschutzgrundverordnung (DSGVO), ist der Datenschutzbeauftragte (DSB) hinsichtlich der Ausübung seiner Tätigkeiten zur Vertraulichkeit und Geheimhaltung verpflichtet.

Welche Partei kann der DSB für Ratschläge konsultieren und ist in diesem Zusammen von seiner Pflicht zur Vertraulichkeit und Geheimhaltung entbunden?

A) Den Vorstand des Unternehmens
B) Die Mitglieder des Datenschutzteams
C) Den Informationssicherheitsbeauftragten (ISB)
D) Die Aufsichtsbehörde

A) Falsch. Die Mitglieder des Vorstands sind zwar leicht zu erreichen, das bedeutet jedoch nicht, dass der DSB diese um Rat bitten sollte. Der DSB erfüllt eine unabhängige Rolle. Die Beratung des Verantwortlichen und des Auftragsverarbeiters zählt zu den primären Aufgaben des DSB. (Literatur A, Kapitel 2 Duties of the DPO, Seite 49. E-Buch, Seite 32. Literatur C DSGVO Art. 39)-BT10
B) Falsch. Die Mitglieder Datenschutzteams sind zwar leicht zu erreichen, das bedeutet jedoch nicht, dass der DSB diese um Rat bitten sollte. Der DSB erfüllt eine unabhängige Rolle. (Literatur A, Kapitel 2 Duties of the DPO, Seite 49. E-Buch, Seite 3. Literatur C DSGVO Art. 39)
C) Falsch. Der Informationssicherheitsbeauftragte ist zwar leicht zu erreichen, das bedeutet jedoch nicht, dass der DSB diesen um Rat bitten sollte. Der DSB erfüllt eine unabhängige Rolle. (Literatur A, Kapitel 2 Duties of the DPO, Seite 49. E-Buch, Seite 32. Literatur C DSGVO Art. 39).
D) Richtig. Die Verpflichtung zu Vertraulichkeit und Geheimhaltung verbietet des dem DSB nicht, die Aufsichtsbehörde zu kontaktieren und um Rat zu bitten. (Literatur D, Abschnitt 4.3)

25 / 40
Sie sind als Datenschutzbeauftragter (DSB) für eine Kaufhauskette im Bereich der Luxusmode tätig. Das Unternehmen hat die Absicht geäussert, eine Gesichtserkennungssoftware erwerben zu wollen, um seine Stammkunden besser identifizieren und bedienen zu können. Alle Kunden, die ein Konto bei der Kaufhauskette haben, sollen über die Änderung informiert werden und erhalten die Möglichkeit zum Opt-Out.

Warum sollten Sie vorab die Durchführung einer Datenschutzfolgeabschätzung (DPIA) empfehlen?

A) Eine Datenschutzfolgeabschätzung ist laut ISO 27001 ein wesentlicher Bestandteil eines Informationssicherheitssystems (ISMS).
B) Die Durchführung einer Datenschutzfolgeabschätzung und deren Unterzeichnung seitens der Geschäftsführung gehört zur guten Praxis, damit das Unternehmen nicht für künftige Zwischenfälle im Bereich der IT-Sicherheit haftbar gemacht werden kann.
C) Laut der DSGVO ist die Durchführung einer Datenschutzfolgeabschätzung verpflichtend, wenn neue Technologien eingesetzt werden, die sich durch Profiling oder Massenüberwachung auf den Schutz der personenbezogenen Daten auswirken können.
D) Laut der DSGVO ist bei jeder Änderung der bestehenden Prozesse, Projekte oder Richtlinien eine Datenschutzfolgeabschätzung erforderlich.

A) Falsch. Die ISO 27001 bezieht sich ganz allgemein auf die Informationssicherheit. Die Notwendigkeit von Datenschutzfolgeabschätzungen wird darin nicht erwähnt.
B) Falsch. Eine Organisation kann und wird für alle Vorfälle, die aufgrund ihrer IT-Strategie eintreten, haftbar gemacht werden. Eine Datenschutzfolgeabschätzung hilft lediglich dabei, auf die relevanten Risiken hinzuweisen.
C) Richtig. Eine Datenschutzfolgeabschätzung gilt als gute Praxis, wenn neue Technologien eingeführt werden und ist in drei Fällen verpflichtend. Das Kaufhaus ist ein öffentlicher Raum, der systematisch mit Hilfe elektronischer Geräte überwacht wird. Bei Entscheidung bezüglich konkreter natürlicher Personen kommt automatisiertes Profiling zum Einsatz. In diesem Fall sind mindestens zwei der drei oben genannten Bedingungen erfüllt. (Literatur A, Kapitel 5 1. Identify the need for a DPIA)
D) Falsch. Eine Datenschutzfolgeabschätzung ist laut der Verordnung nicht immer verpflichtend.

26 / 40
Stellen Sie sich vor, Sie arbeiten für eine grosse Organisation. Ihre Organisation nutzt Software-Tools, mit denen die Mitarbeiter hinsichtlich ihrer Arbeit am Computer leichter überwacht werden können. Die Tools zeigen basierend auf allgemeinen Algorithmen und Zeitangaben an, wann die Mitarbeiter eine Ruhepause benötigen oder sich dehnen sollten. Jetzt will das Unternehmen das Tool um eine Funktionalität erweitern und es an einen Pulsmesser anschliessen, um die Ratschläge bezüglich der Ruhepausen noch besser personalisieren zu können.

Warum müssen Sie eine Datenschutzfolgeabschätzung (DPIA) durchführen?

A) Eine Datenschutzfolgeabschätzung ist bei allen neuen Tools oder Prozessen erforderlich.
B) Das Tool überwacht die Mitarbeiter und umfasst damit die Verarbeitung personenbezogener Daten
C) Es handelt sich um eine neue Anwendung bei der sensible personenbezogene Daten verarbeitet werden.
D) Es handelt sich um eine neue Anwendung mit umfangreicher Überwachung des Verhaltens im öffentlichen Raum.

A) Falsch. Neue Anwendungen beziehungsweise neue Funktionalitäten für bestehende Tools oder Prozesse erfordern nicht immer eine Datenschutzfolgeabschätzung.
B) Falsch. Die Tatsache, dass personenbezogene Daten von Mitarbeitern verarbeitet werden, reicht an sich nicht aus, um eine Datenschutzfolgeabschätzung notwendig zu machen.
C) Richtig. Artikel 35 der DSGVO zur Datenschutzfolgeabschätzung besagt, dass eine DPIA immer dann erforderlich ist, wenn sensible personenbezogene Daten in grossem Umfang verarbeitet werden. Gesundheitsdaten sind sensible Daten. (Literatur A, Kapitel 5 Abschnitt When to conduct a DPIA? E-Buch Seiten 62-63. Literatur C: DSGVO Abschnitt 3, Artikel 35 (3) b und 9(1)).
D) Falsch. Dieser Grund wird zwar in der DSGVO ebenfalls angeführt, trifft hier aber nicht zu, da es sich nicht um einen öffentlichen Raum handelt.

27 / 40
Sie haben gerade Ihren neuen Job als leitender Datenschutzbeauftragter (DSB) im nationalen Verkehrsministerium angetreten. Das Ministerium gibt ein neues Projekt bekannt, das darauf abzielt, das Fahrverhalten der Bürger auf den nationalen Schnellstrassen zu überwachen. Das Ministerium plant den Einsatz eines intelligenten Videoanalysesystems, das automatisch die Nummernschilder einzelner Fahrzeuge erkennt. Eines Morgens kommt die Staatssekretärin in Ihr B üro. Sie will offensichtlich schnell mit dem Projekt beginnen und äussert ihre Sorgen dass Datenschutzfragen zu nicht erwünschten Verzögerungen führen könnten.

Was sollten Sie ihr sagen?

A) Sie sollten sie bitten, sich an die Aufsichtsbehörde zu wenden, da dies eine Frage von nationaler Bedeutung ist, die Ihre Befugnisse ganz klar übersteigt.
B) Sie sollten sie darüber informieren, dass die Art der geplanten Datenverarbeitung, eine Untersuchung mittels Durchführung einer Datenschutzfolgeabschätzung (DPIA) erforderlich macht. Die sich ergebenden Risiken und die Massnahmen zur Verringerung dieser Risiken sollten in den Projektplan integriert werden.
C) Sie informieren sie, dass keine Notwendigkeit für eine Datenschutzfolgeabschätzung (DPIA) besteht, vorausgesetzt die Bürger werden ordnungsgemäss über den Zweck und den Umfang der Datenverarbeitung informiert.
D) Sie sagen ihr, dass das Projekt ernsthaft überdacht werden sollte, da Aktivitäten zur Datenverarbeitung mit 'hohem Risiko' wie Massenüberwachung und Datenverarbeitung zur Erstellung von Profilen laut der DSGVO verboten sind.

A) Falsch. Als leitender Datenschutzbeauftragter sollten Sie hinreichend qualifiziert sein, um Datenschutzfragen auf Ministeriumsebene zu diskutieren.
B) Richtig. Das Projekt umfasst systematische Überwachung sowie innovative Nutzung technologischer Lösungen und erfüllt damit zwei der drei Gründe für die Durchführung einer Datenschutzfolgeabschätzung (DPIA). (Literatur A, Kapitel 5 Identify the need for a DPIA, When to conduct a DPIA)
C) Falsch. Dies befreit eine Organisation nicht von der Verantwortung, die Folgen der geplanten Verarbeitungstätigkeiten für den Schutz personenbezogener Daten abzuschätzen.
D) Falsch. Beobachtung und Überwachung sind nicht an sich verboten, vorausgesetzt die Rechte und Freiheiten der Menschen werden angemessen geschützt.

28 / 40
Die DSGVO spezifiziert lediglich, dass eine Datenschutzfolgeabschätzung (DPIA) in bestimmten Situationen durchgeführt werden muss. Sie schreibt Ihnen jedoch nicht vor, *wie* Sie diese tatsächlich durchzuführen haben. Dennoch spezifiziert die Verordnung einige Mindestanforderungen an die Datenschutzfolgeabschätzung (DPIA).

Welche Aktivität sollte angesichts dieser Mindestanforderungen **immer** Teil einer Datenschutzfolgeabschätzung (DPIA) sein?

A) Die Erarbeitung eines Verfahrens bezüglich des Auskunftsrechts betroffener Personen, um die Rechte der betroffenen Personen zu wahren
B) Die Identifizierung der verarbeiteten personenbezogenen Daten und der Zweck der Verarbeitung
C) Die Benachrichtigung der betroffenen Personen, dass eine Bewertung stattfinden wird und die Anforderung ihrer ausdrücklichen Einwilligung
D) Die Erarbeitung eines Notfallplans und die Festlegung angemessener Sicherheitsmassnahmen, um Verletzungen des Schutzes personenbezogener Daten zu vermeiden

A) Falsch. Dies ist eine mögliche Massnahme, die sich aufgrund einer Datenschutzfolgeabschätzung ergeben kann. Es ist jedoch keine standardmässige Stufe oder Aktivität im Rahmen einer Datenschutzfolgeabschätzung.
B) Richtig. Datenmapping ist ein wichtiger Bestandteil jeder Datenschutzfolgeabschätzung. Zuerst mü ssen die von Ihnen erhobenen und verarbeiteten Daten identifiziert und verstanden werden. (Literatur A, Kapitel 8 Objectives and outcomes, Five key stages of the DPIA).
C) Falsch. Für eine Datenschutzfolgeabschätzung ist keine Einwilligung der betroffenen Personen erforderlich. Eine Datenschutzfolgeabschätzung stellt kein weiteres Risiko bezüglich der personenbezogenen Daten dar, sondern zielt darauf ab, die Risiken zu bewerten und zu reduzieren.
D) Falsch. Die Festlegung der entsprechenden Notfallstrategien für Verletzungen personenbezogener Daten ist eine Massnahme, die sich aufgrund einer Datenschutzfolgeabschätzung ergeben kann. Es ist jedoch keine standardmässige Stufe oder Aktivität im Rahmen einer Datenschutzfolgeabschätzung.

29 / 40
Ein Unternehmen hat den Entschluss gefasst, seine Kundendaten besser zu nutzen, um Trends entdecken und analysieren und bessere Prognosen erstellen zu können. Dazu soll eine neue Unternehmenseinheit aufgebaut werden. Die Datenspezialisten werden mit Hilfe der neuesten Tools für die Datenanalyse ein Data Warehouse einführen.

Sie sind der Datenschutzbeauftragte (DSB) und haben ernsthafte Bedenken geäussert, da es sich hierbei um ein hoch riskantes Unterfangen handelt, dass sich negativ auf die Rechte der betroffenen Personen auswirken kann. Sowohl der CIO als auch der CEO wollen die Entwicklungen jedoch fortführen und scheinen nicht auf Ihre Bedenken reagieren zu wollen.

Wie gehen Sie in einem solchen Fall am **besten** vor?

A) Sie führen eine Datenschutzfolgeabschätzung (DPIA) durch und besprechen das Ergebnis und die möglichen Massnahmen zur Eindämmung des Risikos mit dem Vorstand und den anderen Stakeholdern.
B) Sie beteiligen den CIO an der Datenanonymisierung damit die DSGVO nicht mehr greift.
C) Sie richten eine Kundenumfrage ein, um sich direkt an die Kunden zu wenden und deren ausdrückliche Einwilligung für diese Verarbeitung ihrer personenbezogenen Daten einzuholen.
D) Sie wenden sich an die Aufsichtsbehörde, holen deren Meinung zu der geplanten Verarbeitung personenbezogener Daten ein und bitten die Behörde um Unterstützung bei der Erläuterung der Risiken.

A) Richtig. Zuerst müssen Sie die Risiken der Verarbeitung der personenbezogenen Daten beurteilen. Sind die Risiken hoch, so können je nach Risikobereitschaft des Unternehmens diverse Massnahmen ergriffen werden. (Literatur A, Kapitel 8, Abschnitt: Consultation und Kapitel 5, Abschnitt: Privacy impact assessments, Schritt 1. Identify the need for a PIA and paragraph When to conduct a DPIA)
B) Falsch. Die Anonymisierung und Pseudonymisierung von Daten mag eine Massnahme zur Eindämmung der Risiken sein, zuerst aber müssen die Risiken mit Hilfe einer Datenschutzfolgeabschätzung ermittelt werden. Darüber hinaus ist für die Anonymisierung von Daten ein Rechtsgrund erforderlich, da es sich hierbei ebenfalls um eine Verarbeitungstätigkeit handelt.
C) Falsch. Eine ausdrückliche Einwilligung ist keine Legitimation für Verarbeitungstätigkeiten, die gegen Datenschutzprinzipien, wie zum Beispiel Zweckbindung und Datenminimierung, verstossen.
D) Falsch. Zuerst müssen Sie die Risiken der Verarbeitung der personenbezogenen Daten beurteilen. Sind die Risiken gering oder können angemessene Massnahmen ergriffen werden, um diese Risiken zu reduzieren, dann müssen Sie sich nicht an die Aufsichtsbehörden wenden (Datenschutzbehörde).

30 / 40
Warum kann eine Datenschutzfolgeabschätzung (DPIA) als Teil des Risikomanagements einer Organisation betrachtet werden?

A) Eine Datenschutzfolgeabschätzung dient der Identifizierung von Risiken für betroffene Personen, die von der Organisation eingedämmt werden müssen.
B) Eine Datenschutzfolgeabschätzung dient der Identifizierung von Risiken für die Organisation, die von der Organisation eingedämmt werden müssen.
C) Eine Datenschutzfolgeabschätzung dient der Abschätzung der Folgen und dies ist für die Risikokategorisierung erforderlich.
D) Eine Organisation muss zur Konformität (Compliance) mit der DSGVO eine Datenschutzfolgeabschätzung durchführen.

A) Richtig. (Literatur A, Kapitel 6, Abschnitt: DPIAs as part of risk management)
B) Falsch. Eine Datenschutzfolgeabschätzung konzentriert sich auf die Folgen für den Schutz personenbezogener Daten.
C) Falsch. Dies ist ein Ansatz der Informationssicherheit, bei dem das Risiko mit Hilfe der Formel Schwere x Wahrscheinlichkeit berechnet wird. Dies ist jedoch nicht das Ziel der Datenschutzfolgeabschätzung.
D) Falsch. Eine Datenschutzfolgeabschätzung ist nicht immer erforderlich, sondern nur bei neuen Verarbeitungsaktivitäten, Technologien oder hohen Risiken. (Literatur C DSGVO Art. 35). Konformität ist auch ohne Durchführung einer Datenschutzfolgeabschätzung möglich.

31 / 40
Wichtig im Rahmen einer Datenschutzfolgeabschätzung (DPIA) ist die Bewertung der Risiken für den Datenschutz. Der nächste Schritt besteht darin, diese Risiken zu eliminieren oder auf ein annehmbares Mass (Risikoreaktion) zu reduzieren.

Bei welcher Massnahme handelt es sich um eine typische Risikoreaktion?

A) Die Festlegung von Kennzahlen zur Messung der Wirksamkeit
B) Die Reduzierung der Menge an erhobenen Daten
C) Die Einführung eines Datenschutzrisikoregisters
D) Die Freigabe und Aufzeichnung der Ergebnisse einer Datenschutzfolgeabschätzung (DPIA)

A) Falsch. Dies ist keine Reaktion zur Risikoeindämmung.
B) Richtig. Das ist eine sinnvolle Reaktion auf ein Risiko und reduziert die möglichen Folgen einer Verletzung des Schutzes personenbezogener Daten. (Literatur A, Kapitel 8 Five key stages of the DPIA)
C) Falsch. Dies ist keine Reaktion zur Risikoeindämmung.
D) Falsch. Dies ist keine Reaktion zur Risikoeindämmung.

32 / 40
Muss eine Datenschutzfolgeabschätzung (DPIA) durchgeführt werden, so sind laut der DSGVO mehrere Grundsätze zu beachten. Zwei dieser Grundsätze sind die Bewertung der Verhältnismässigkeit und der Notwendigkeit, sowie eine Bewertung der zur Bewältigung der identifizierten Risiken geplanten Abhilfemassnahmen.

Welches weitere Element muss laut DSGVO in einer Datenschutzfolgeabschätzung enthalten sein?

A) Ein Protokoll, wie im Falle von Verletzungen des Schutzes personenbezogener Daten zu verfahren ist
B) Ein öffentlicher Bericht über das Ergebnis der Datenschutzfolgeabschätzung
C) Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

A) Falsch. Es gibt keine offizielle Forderung für ein Protokoll bei Verletzungen des Schutzes personenbezogener Daten und falls doch wäre es nicht Teil der Datenschutzfolgeabschätzung.
B) Falsch. Die DSGVO fordert keinen öffentlichen Bericht über das Ergebnis, obwohl dies in Literatur A, Kapitel 8: Five key stages erwähnt wird.
C) Richtig. Dieses Element wird in Literatur C: DSGVO, Abschnitt 3, Artikel 35 (7) erwähnt. (Literatur A, Kapitel 5 Privacy Impact Assessments und Kapitel 8 Five key stages of the DPIA. Literatur E: Kapitel III. Abschnitt C How to carry out a DPIA?)

33 / 40
Sie sind in Ihrer Organisation für ein Projekt verantwortlich, bei dem auch personenbezogene Daten verarbeitet werden. Im Rahmen Ihrer Verantwortung entscheiden Sie eine Datenschutzfolgeabschätzung (DPIA) durchzuführen und mit dem Datenmapping zu beginnen.

Warum ist das Datenmapping ein sinnvoller Bestandteil des DPIA-Verfahrens?

A) Durch das Datenmapping verschafft man sich einen Überblick über die Risiken für personenbezogene Daten
B) Durch das Datenmapping verschafft man sich einen Überblick über die bei der Verarbeitung personenbezogener Daten eingesetzten Systeme
C) Das Datenmapping trägt dazu bei, den Zweck der Datenverarbeitung zu identifizieren

A) Richtig. (Literatur A, Kapitel 7, Data mapping, DPIAs and risk management und Literatur C DSGVO Artikel 35 (1))
B) Falsch. Dies ist Teil des erforderlichen Verzeichnisses von Verarbeitungstätigkeiten (Artikel 30 DSGVO).
C) Falsch. Dies muss ermittelt werden, bevor die Datenschutzfolgeabschätzung (DPIA) stattfinden kann und lässt sich nicht vom Datenmapping ableiten.

34 / 40
Eine Organisation fällt bezüglich ihrer Kunden automatisierte Entscheidungen, die auf Profiling basieren.

Welcher Aspekt einer Datenschutzfolgeabschätzung (DPIA) ist in diesem Fall am **meisten** zu beachten?

A) Die Bewertung, ob für diese Verarbeitungstätigkeit eine Datenschutzfolgeabschätzung durchgeführt werden muss
B) Die Bewertung, wann die Daten gelöscht werden
C) Massnahmen zum Schutz der Rechte der betroffenen Personen durch das Ermöglichen menschlichen Eingreifens
D) Massnahmen, die der Sicherheit der Daten dienen und verhindern, dass die betroffenen Personen Zugriff auf diese erhalten

A) Falsch. Bei Verarbeitungstätigkeiten mit automatisierten Entscheidungen, einschliesslich Profiling, ist stets eine Datenschutzfolgeabschätzung erforderlich (DSGVO, Artikel 35 (3) a). Die Notwendigkeit der Durchführung einer Datenschutzfolgeabschätzung versteht sich damit von selbst.
B) Falsch. Dies ist zwar Teil des Verfahrens zur Datenschutzfolgeabschätzung, muss jedoch in diesem Fall nicht am stärksten beachtet werden. Möglicherweise ist es jedoch erforderlich, Daten länger aufzubewahren, um automatisierte Entscheidungen prüfen zu können, sollten diese angefochten werden.
C) Richtig. Literatur E: Kapitel III. Abschnitt C How to carry out a DPIA?. Literatur C DSGVO, Artikel 22(3) nennt dies als Anforderung Literatur A, Kapitel 5, Privacy Impact Assessments und When to conduct a DPIA.
D) Falsch. Daten müssen allgemein zwar gesichert werden, aber die betroffenen Personen haben ein Auskunftsrecht (DSGVO, Artikel 15).

35 / 40
Sie sind in Ihrer Organisation für eine Datenschutzfolgeabschätzung (DPIA) verantwortlich. Im Zusammenhang mit dieser Datenschutzfolgeabschätzung konsultieren Sie eine Reihe von Kollegen, um eine ordnungsgemässe Beschreibung der für die Datenverarbeitung geplanten Tätigkeiten und Zwecke zu erstellen. Im Laufe dieser Konsultation zeigt sich, dass bei der Verarbeitung anscheinend personenbezogene Daten erhoben werden, die zwar für die aktuellen Zwecke nicht unbedingt erforderlich sind, sich für zukünftige Zwecke jedoch als nützlich erweisen könnten. Die Erhebung dieser Daten mit dem aktuellen Prozess zu verbinden ist effizienter.

Was sollten Sie in dieser Situation tun?

A) Sie sollten die Verarbeitung zulassen, weil Effizienz ein legitimes Interesse Ihrer Organisation entsprechend Artikel 6 der DSGVO darstellt.
B) Sie sollten fordern, dass die zusätzlichen Daten nicht mehr erhoben werden, da sie für den Zweck der Datenverarbeitung, für die die Datenschutzfolgeabschätzung durchgeführt wird, nicht erforderlich sind.
C) Sie sollten fordern, dass die Kollegen Ihnen einen legitimen Rechtsgrund für die Verarbeitung der zusätzlichen Daten entsprechend Artikel 6 der DSGVO bieten und die Verarbeitung zulassen.
D) Sie sollten fordern, dass die Daten entsprechend gesichert werden, um eine Verletzung des Schutzes personenbezogener Daten zu verhindern.

A) Falsch. Ihr legitimes Interesse ist zwar ein legitimer Grund für die Verarbeitung, aber dennoch muss vor der Verarbeitung ein festgelegter und eindeutiger Zweck vorliegen.
B) Richtig. Dies entspricht dem Prinzip der Prüfung der Notwendigkeit und Verhältnismässigkeit der Verarbeitung personenbezogener Daten. (Literatur E, Kapitel III., Abschnitt C How to carry out a DPIA? Literatur C. DSGVO, Artikel 35(7)b. Zusätzlich: Literatur A, Kapitel 5 Introduction und Kapitel 8 Objectives and outcomes).
C) Falsch. Personenbezogene Daten dürfen nur für festgelegte und eindeutige Zwecke verarbeitet werden (DSGVO, Artikel 5 (1) b)). Ohne Vorliegen eines Zwecks gibt es keinen legitimen Grund für die Verarbeitung gemäss Artikel 6, DSGVO.
D) Falsch. Die unrechtmässige Verarbeitung der personenbezogenen Daten stellt schon an sich eine Verletzung des Schutzes personenbezogener Daten dar.

36 / 40
Sie führen für einen neuen Service Ihres Unternehmens, bei dem personenbezogene Daten der Kunden in grossem Umfang verarbeitet werden, eine Datenschutzfolgeabschätzung (DPIA) durch. F ür die Verarbeitung liegen berechtigte Gründe und ein festgelegter, eindeutiger Zweck vor. Ausserdem werden geeignete Massnahmen umgesetzt, um die Risiken für die Rechte der betroffenen Personen abzumildern. Es ist jedoch klar, dass der Service nur Erfolg haben wird, wenn er von den Kunden akzeptiert wird.

Welche spezifische Massnahme sollten Sie bezüglich des Verfahrens der Datenschutzfolgeabschätzung in diesem spezifischen Fall ergreifen?

A) Sie sollten sich an die Kunden oder deren Vertreter wenden und deren Meinung zur Verarbeitung ihrer personenbezogenen Daten einholen
B) Sie sollten sich an die Aufsichtsbehörde wenden und sich die Rechtmässigkeit der Verarbeitung bestätigen lassen
C) Sie sollten einen Helpdesk einrichten, an den sich Kunden wenden und sich den Service nach dem Rollout erklären lassen können
D) Sie sollten einen Bericht über die Datenschutzfolgeabschätzung an die Kunden senden, um diesen zu versichern, dass Massnahmen zur Abminderung des Risikos ergriffen wurden

A) Richtig. (Literatur C DSGVO Artikel 35 (9) Literatur A, Kapitel 8, Abschnitt: Consultation)
B) Falsch. Die Datenschutzbehörde vertritt nicht die Kunden und Rechtmässigkeit impliziert an sich noch keine Akzeptanz.
C) Falsch. Dies ist nicht Teil des Verfahrens zur Datenschutzfolgeabschätzung.
D) Falsch. Dies ist so oder so Pflicht und nicht Teil des Verfahrens zur Datenschutzfolgeabschätzung.

37 / 40
Sie arbeiten als Datenschutzbeauftragter (DSB) in einem grossen Logistikunternehmen mit internationaler Kundschaft. Der Leiter der Personalabteilung berichtet, dass er einen verschlü sselten USB-Stick mit den Mitarbeiterdaten von 35 Mitarbeitern verlegt oder verloren hat.

Warum ist dies unter der DSGVO als Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden?

A) Ein Sicherheitsvorfall, der mit einem Verlust an vertraulichen Unternehmendaten einhergeht, ist als Verletzung des Schutzes personenbezogener Daten zu melden.
B) Der Vorfall ist zu melden, weil der Verlust eines Geräts mit personenbezogenen Daten ein Risiko für die Rechte und Freiheiten der natürlichen Personen darstellt.
C) Der Vorfall ist unverzüglich zu melden, damit die Aufsichtsbehörde die 35 Mitarbeiter über die Verletzung des Schutzes ihrer personenbezogenen Daten informieren kann.

A) Falsch. Nur Sicherheitsvorfälle mit *personenbezogenen Daten*gelten als Verletzung des Schutzes personenbezogener Daten gemäss der Definition in der DSGVO.
B) Richtig. Der Verlust eines Geräts stellt eine Sicherheitslücke dar. Das Gerät ist zwar ausreichend geschützt, aber im Falle böswilliger Absicht besteht das Risiko, dass die Daten gefährdet sind. Dies stellt eine Verletzung des Schutzes personenbezogener Daten dar und ist der Aufsichtsbehörde zu melden. (Literatur A, Kapitel 3 Anatomy of a data breach, Kapitel14 Notification)
C) Falsch. Die Aufsichtsbehörde ist nicht dafür verantwortlich, den Vorfall an die betroffenen Stakeholder zu melden.

38 / 40
Wann muss eine Organisation die Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde melden?

A) Immer dann, wenn ein Vorfall wahrscheinlich mit einem Risiko für die Rechte und Freiheiten der betroffenen Personen einhergeht
B) Immer dann, wenn eine Bedrohung der Sicherheit die Rechte und Freiheiten der betroffenen Personen gefährdet
C) Nur dann, wenn eine Organisation nicht in der Lage ist, den Vorfall innerhalb von 72 Stunden ab Eintreten zu lösen
D) Nur dann, wenn der Vorfall innerhalb von 72 Stunden ab Eintreten erkannt wird

A) Richtig. Eine Meldung an die Aufsichtsbehörde ist bei allen Vorfällen mit personenbezogenen Daten erforderlich. (Literatur A, Kapitel 14, Abschnitt Notification)
B) Falsch. Eine Bedrohung an sich reicht nicht aus Phishing beispielsweise gilt allgemein als Bedrohung. Eine Meldung an die Aufsichtsbehörde ist jedoch nur erforderlich, wenn eine Sicherheitslücke in Form eines tatsächlichen Vorfalls vorliegt.
C) Falsch. Die Lösung des Vorfalls sollte die Meldung an die Aufsichtsbehörde nicht verzögern (“schnellstmöglich”).
D) Falsch. Der Incident Management Prozess kann das Risiko möglicherweise nicht innerhalb von 72 Stunden erkennen. Das kann länger dauern. Darum schreibt die Verordnung Folgendes vor: “unverzü glich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde”.

39 / 40
Wann muss eine Organisation die Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen melden?

A) Immer dann, wenn eine Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem 'hohen Risiko' für die Rechte und Freiheiten der betroffenen Personen führt.
B) Immer dann, wenn ein Sicherheitsvorfall die Rechte und Freiheiten der betroffenen Personen gefährdet.
C) Nur wenn die Aufsichtsbehörde es als erforderlich erachtet, dass die betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten informiert werden.
D) Nur bei böswilliger Absicht, wenn personenbezogene Daten durch externe Akteure, wie zum Beispiel Cyberkriminelle gefährdet werden.

A) Richtig. Betroffene Personen sollten nur informiert werden, wenn die Verletzung personenbezogener Daten ein 'hohes Risiko' für die Rechte und Freiheiten der persönlichen Personen darstellt. (Literatur A, Kapitel 14, Notifications)
B) Falsch. Die Benachrichtigung der betroffenen Personen ist nur bei Sicherheitsvorfällen mit 'hohem Risiko' erforderlich.
C) Falsch. Eine Organisation muss die Interessen des Unternehmens und die Interessen der betroffenen Personen bei der Entscheidung, ob die betroffenen Personen über eine Sicherheitsverletzung informiert werden sollen, sorgfältig abwägen.
D) Falsch. Die Meldung richtet sich nicht nach der zugrundeliegenden Ursache oder Absicht der Sicherheitsverletzung. Eine Verletzung des Schutzes personenbezogener Daten kann sowohl böswillig und absichtlich als auch versehentlich verursacht werden.

40 / 40
Jede Organisation wird immer wieder mit Verletzungen des Schutzes personenbezogener Daten zu tun haben, die an die Aufsichtsbehörde zu melden sind. Da der Meldeprozess immer wieder durchzuführen ist, empfiehlt es sich eine Meldevorlage anzufertigen, die folgende Punkte umfasst:

- die Art der Verletzung des Schutzes personenbezogener Daten
- die wahrscheinlichen Folgen
- die Massnahmen zur Eindämmung dieser Folgen

Welche weiteren Elementen sollten in der Vorlage enthalten sein?

A) - der Name und die Kontaktdaten des CEO
- der Notfallmanagementplan

B) - die Zahl der betroffenen Personen
- den Namen der Person, die für die Verletzung des Schutzes personenbezogener Daten verantwortlich ist.

C) - die Zahl der betroffenen Personen
- den Namen und die Kontaktdaten des Datenschutzbeauftragten und anderer Kontaktstellen

D) - die Nummer des Sicherheitsvorfalls
- die Analyse der Bedrohungen der Cybersicherheit

A) Falsch. Der CEO hat mit der Meldung der Verletzung des Schutzes personenbezogener Daten nichts zu tun. Auch der Notfallmanagementplant sollte nicht gemeldet werden. Letzterer wird nur im Falle eines Audits von der Aufsichtsbehörde bewertet.

B) Falsch. Die Aufsichtsbehörde ist nicht an den Namen der Personen interessiert, die in den Vorfall involviert waren oder von diesem betroffen sind. Die Meldung führt nicht zu Bestrafungen.

C) Richtig. Diese Elemente sollte in einer Meldung an die Aufsichtsbehörde enthalten sein (Literatur A, Kapitel 14 Notification)

D) Falsch. Diese Elemente müssen nicht gemeldet werden.

Beurteilung

Die richtigen Antworten auf die Fragen in diesem Musterexamen finden Sie in nachstehender Tabelle.

Frage	Antwort	Frage	Antwort
1	A	**21**	B
2	A	**22**	D
3	A	**23**	A
4	B	**24**	D
5	C	**25**	C
6	A	**26**	C
7	B	**27**	B
8	B	**28**	B
9	B	**29**	A
10	B	**30**	A
11	B	**31**	B
12	A	**32**	C
13	C	**33**	A
14	C	**34**	C
15	B	**35**	B
16	C	**36**	A
17	B	**37**	B
18	C	**38**	A
19	A	**39**	A
20	C	**40**	C

Kontakt EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER