Musterprüfung

Ausgabe 201805

Copyright © EXIN Holding B.V. 2018. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Inhalt

Einführung

Dies ist die Musterprüfung EXIN Privacy and Data Protection Foundation (PDPF.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 60 Minuten.

Viel Erfolg!

Musterprüfung

1 / 40
Die rechtswidrige Erhebung, Speicherung, Änderung, Offenlegung oder Verbreitung personenbezogener Daten ist nach europäischem Recht strafbar.

Um was für eine Art von Straftat handelt es sich?

A) Eine inhaltsbezogene Straftat
B) Eine Wirtschaftsstraftat
C) Eine Straftat in Bezug auf geistiges Eigentum
D) Eine Straftat in Bezug auf die Privatsphäre

2 / 40
In welchem Zusammenhang stehen Privatsphäre und Datenschutz?

A) Datenschutz ist eine Teilmenge der Privatsphäre.
B) Privatsphäre ist eine Teilmenge des Datenschutzes.
C) Die Begriffe bezeichnen dasselbe.
D) Es gibt keine Privatsphäre ohne Datenschutz.

3 / 40
Welchen **Hauptzweck** hat die Datenschutz-Grundverordnung (DSGVO)?

A) Eine gemeinsame Grundlage bilden, auf der die Mitgliedstaaten ihre eigenen Gesetze aufbauen können.
B) Nicht-EU-Länder dazu verpflichten, das Recht von Einzelpersonen aus der EU auf Privatsphäre zu achten.
C) Privatsphäre als grundlegendes Menschenrecht für alle gewährleisten.
D) Den Datenschutz für Einzelpersonen innerhalb der EU stärken und vereinheitlichen.

4 / 40
Die Datenschutz-Grundverordnung (DSGVO) bezieht sich auf den Schutz personenbezogener Daten.

Wie lautet die Definition personenbezogener Daten?

A) Alle Informationen über eine identifizierte oder identifizierbare natürliche Person
B) Alle Informationen, die europäische Bürgerinnen und Bürger schützen möchten
C) Daten, aus denen die rassische und ethnische Herkunft oder religiöse Überzeugungen direkt oder indirekt hervorgehen, sowie Daten zur Gesundheit oder zur sexuellen Orientierung
D) Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

5 / 40
Welche Kategorie personenbezogener Daten wird nach der Datenschutz-Grundverordnung (DSGVO) als sensible Daten erachtet?

A) Kreditkarteninformationen
B) Sozialversicherungsnummer
C) Ausweisnummer
D) Gewerkschaftsmitgliedschaft

6 / 40
Wie lautet die Definition von „Verarbeitung“ personenbezogener Daten nach der Datenschutz-Grundverordnung (DSGVO)?

A) Jeder Vorgang im Zusammenhang mit personenbezogenen Daten
B) Jeder Vorgang im Zusammenhang mit personenbezogenen Daten, mit Ausnahme der Löschung und Vernichtung
C) Nur Vorgänge, bei denen Daten in den sozialen Medien geteilt oder per E-Mail oder anderweitig über das Internet weitergegeben werden
D) Nur Vorgänge, bei denen personenbezogene Daten für die Zwecke verwendet werden, für die sie erhoben wurden

7 / 40
Eine unabhängige Behörde, die von einem Mitgliedstaat gemäß Artikel 51 eingerichtet wurde.

Welche Rolle im Datenschutz ist definiert?

A) Verantwortlicher
B) Auftragsverarbeiter
C) Aufsichtsbehörde
D) Dritter

8 / 40
„Informierte Einwilligung“ ist eine rechtmäßige Grundlage für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung (DSGVO). Der Zweck der Verarbeitung, für die die Einwilligung erteilt wird, muss dokumentiert werden.

Zu welchem Zeitpunkt sollte die Einwilligung der betroffenen Person eingeholt werden?

A) Nachdem die Zweckbestimmung dargelegt wurde und bevor personenbezogene Daten erhoben werden.
B) Bevor die Zweckbestimmung ausgearbeitet und dargelegt wird.
C) Bevor die personenbezogenen Daten verarbeitet werden.
D) Bevor die personenbezogenen Daten veröffentlicht oder verbreitet werden.

9 / 40
Die Datenschutz-Grundverordnung (DSGVO) basiert auf den Grundsätzen der Verhältnismäßigkeit und der Subsidiarität.

Was bedeutet „Verhältnismäßigkeit“ in diesem Zusammenhang?

A) Personenbezogene Daten können nur entsprechend der Zweckbestimmung verarbeitet werden.
B) Personenbezogene Daten können ohne ausdrückliche und informierte Einwilligung nicht wiederverwendet werden.
C) Personenbezogene Daten dürfen nur verarbeitet werden, wenn es keine anderen Mittel gibt, um die Zwecke zu erreichen.
D) Personenbezogene Daten müssen in Bezug auf die Zwecke angemessen und relevant sein und sich im Rahmen halten.

10 / 40
Die Verarbeitung personenbezogener Daten muss den allgemeinen Qualitätsvorschriften entsprechen.

Was ist eine der in der Datenschutz-Grundverordnung (DSGVO) definierten Vorschriften?

A) Die verarbeiteten Daten müssen archiviert werden.
B) Die verarbeiteten Daten müssen verschlüsselt werden.
C) Die verarbeiteten Daten müssen indiziert werden.
D) Die verarbeiteten Daten müssen relevant sein.

11 / 40
Jedes Mal, wenn personenbezogene Daten verarbeitet werden, müssen Verhältnismäßigkeit und Subsidiarität geprüft werden.

Was ist eine Anforderung an die Verarbeitung personenbezogener Daten?

A) Sie muss von der kleinstmöglichen Anzahl von Mitarbeitern vorgenommen werden, die für den Verantwortlichen oder ein verbundenes Unternehmen arbeiten.
B) Sie muss immer auf das für die Zielerreichung Notwendige, und auf die am wenigsten „in die Privatsphäre eingreifenden“ Daten beschränkt sein.
C) Sie muss auf eine vordefinierte Speichergröße beschränkt sein, und das verwendete System muss von dem Verantwortlichen finanziert werden.
D) Sie muss für die kleinstmögliche Anzahl von Zwecken verwendet werden und darf nicht außerhalb der Räumlichkeiten des Auftragsverarbeiters erfolgen.

12 / 40
Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass (...) nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck der Verarbeitung erforderlich sind.

Welcher Begriff ist in der Datenschutz-Grundverordnung (DSGVO) definiert?

A) Einhaltung
B) Datenschutz durch datenschutzfreundliche Voreinstellungen
C) Datenschutz durch Technikgestaltung
D) Eingebetteter Schutz

13 / 40
Wie lautet der Begriff für die unbefugte Weitergabe von oder den unbefugten Zugriff auf personenbezogene(n) Daten in der Datenschutz-Grundverordnung (DSGVO)?

A) Verletzung der Geheimhaltungspflicht
B) Verletzung des Schutzes personenbezogener Daten
C) Zwischenfall
D) Sicherheitsvorfall

14 / 40
Es wurde festgestellt, dass es zu einer Verletzung des Schutzes sensibler personenbezogener Daten gekommen ist.

Wem muss diese Verletzung letztendlich nach der Datenschutz-Grundverordnung (DSGVO) gemeldet werden?

A) Dem Datenschutzbeauftragten
B) Der Aufsichtsbehörde
C) Dem Abteilungsleiter
D) Der Polizei

15 / 40
Bei der Erstellung einer Sicherungskopie stürzt eine Server-Festplatte ab. Sowohl die Daten als auch die Sicherungskopie gehen verloren. Die Festplatte enthielt personenbezogene Daten, aber keine sensiblen Daten.

Um was für einen Zwischenfall handelt es sich?

A) Verletzung des Schutzes personenbezogener Daten
B) Verletzung der Sicherheit
C) Sicherheitsvorfall

16 / 40
Eine Person, die für eine Gewerkschaft arbeitet, hat einen Newsletter-Entwurf mit nach Hause genommen, um ihn dort für die Mitglieder fertigzustellen. Der USB-Stick mit dem Entwurf und der Mailingliste ist verloren gegangen.

Wem muss diese Verletzung des Schutzes personenbezogener Daten neben der Datenschutzbehörde noch gemeldet werden?

A) Allen Mitgliedern auf der Mailingliste
B) Den Gewerkschaftsmitarbeitern
C) Der Polizei

17 / 40
Eine Organisation für Sozialdienste plant, eine neue Datenbank zu entwickeln, um ihre Kunden und deren Pflegebedarf zu verwalten.

Worin besteht einer der ersten wichtigen Schritte, um eine Genehmigung der Aufsichtsbehörde zu beantragen?

A) Daten über die Kunden und die Menge und Art der benötigten und erbrachten Pflegeleistungen erheben.
B) Eine Datenschutz-Folgenabschätzung (DPIA) zur Bewertung der Risiken der beabsichtigten Verarbeitung durchführen.
C) Die Einwilligung der Kunden für die beabsichtigte Verarbeitung ihrer personenbezogenen Daten einholen.

18 / 40
In welchem Fall müssen die betroffenen Personen immer über eine Verletzung des Schutzes personenbezogener Daten informiert werden?

A) Die personenbezogenen Daten wurden in einer Einrichtung des Auftragsverarbeiters verarbeitet, die sich außerhalb der EU befindet.
B) Die personenbezogenen Daten wurden von einer Partei verarbeitet, die zwar dem Entwurf des vom Verantwortlichen vorgelegten Vertrags zur Auftragsverarbeitung zugestimmt, diesen aber noch nicht verbindlich unterzeichnet hat.
C) Das System, auf dem die personenbezogenen Daten verarbeitet wurden, wurde angegriffen und die Speichermedien des Systems wurden bei dem Angriff beschädigt.

19 / 40
Ein niederländischer Verantwortlicher hat die Verarbeitung sensibler personenbezogener Daten an einen Auftragsverarbeiter in einem nordafrikanischen Land vergeben, ohne die Aufsichtsbehörde zu konsultieren. Dies wurde aufgedeckt und von der Aufsichtsbehörde bestraft.

Sechs Monate später stellt die Aufsichtsbehörde fest, dass sich der Verantwortliche des gleichen Verstoßes bei einem anderen Verarbeitungsvorgang schuldig gemacht hat.

Was ist das maximale Bußgeld, das die Aufsichtsbehörde in diesem Fall verhängen kann?

A) € 750.000
B) € 1.230.000
C) € 10.000.000 oder 2 % des weltweiten Umsatzes des Unternehmens, je nachdem, was höher ist
D) € 20.000.000 oder 4 % des weltweiten Umsatzes des Unternehmens, je nachdem, was höher ist

20 / 40
Den Aufsichtsbehörden ist eine Reihe von Pflichten auferlegt, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten.

Was ist eine dieser Pflichten?

A) Beurteilung von Verhaltenskodizes für bestimmte Sektoren in Bezug auf die Verarbeitung personenbezogener Daten.
B) Festlegung eines Mindestmaßes von Maßnahmen zum Schutz personenbezogener Daten.
C) Untersuchung aller Verletzungen des Schutzes personenbezogener Daten, die ihnen gemeldet wurden.
D) Überprüfung der Verträge und verbindlichen internen Datenschutzvorschriften auf die Einhaltung der Bestimmungen.

21 / 40
Eine religiöse Vereinigung möchte personenbezogene Daten an ihre religiöse Autorität in einem außereuropäischen Land weitergeben, um eine rechtliche Anforderung der betreffenden Regierung einzuhalten.

Welche Bestimmung der Datenschutz-Grundverordnung (DSGVO) gilt in diesem Fall?

A) Als Ausnahmeregelung ist einer religiösen Vereinigung die Verarbeitung sensibler Daten, aus denen religiöse Überzeugungen hervorgehen, gestattet.
B) Es ist rechtlich nicht zulässig, personenbezogene Daten aus der EU als Reaktion auf eine rechtliche Anforderung eines Drittlandes zu übermitteln.
C) Die Verarbeitung ist rechtlich zulässig, sofern eine spezifische und eindeutige Einwilligung der betroffenen Person eingeholt wurde.
D) Die Verarbeitung personenbezogener Daten außerhalb der EU ist nach den von der EU-Kommission ausgearbeiteten Standartvertragsklauseln zulässig.

22 / 40
Am 12. Juli 2016 hat die Europäische Kommission eine Entscheidung über die Übermittlung personenbezogener Daten mit den USA (EU-US-Datenschutzschild) umgesetzt.

Welche Art von Entscheidung ist dies im Sinne der Datenschutz-Grundverordnung (DSGVO)?

A) Ein Angemessenheitsbeschluss
B) Ein Ausnahmeerlass
C) Ein verbindlicher Standardvertrag
D) Ein die DSGVO ersetzendes Abkommen

23 / 40
Verbindliche interne Datenschutzvorschriften dienen Organisationen als Mittel, um ihren administrativen Aufwand hinsichtlich der Einhaltung der Datenschutz-Grundverordnung (DSGVO) zu reduzieren.

Inwiefern helfen ihnen diese Vorschriften?

A) Sie ermöglichen ihnen, unterstützende Verträge mit allen Beteiligten im Ausland abzuschließen.
B) Sie ermöglichen ihnen, personenbezogene Daten durch Dritte außerhalb des Europäischen Wirtschaftsraums (EWR) verarbeiten zu lassen.
C) Sie vermeiden die Notwendigkeit, jede Aufsichtsbehörde in dem EWR einzeln informieren zu müssen.
D) Sie verhindern, dass sie von einer Aufsichtsbehörde die Genehmigung zur Verarbeitung der Daten einholen müssen, sobald ihre verbindlichen internen Datenschutzvorschriften akzeptiert wurden.

24 / 40
Falls ein Auftragnehmer die Verarbeitung personenbezogener Daten an eine andere Partei abgibt, schließen die Parteien einen schriftlichen Vertrag. Dieser Vertrag legt den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen fest.

Welcher andere Aspekt muss durch diesen schriftlichen Vertrag geregelt werden?

A) Die Rechenschaftspflicht des Auftragsverarbeiters
B) Die Meldepflicht im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten
C) Die Pflichten und Rechte des Verantwortlichen
D) Die Pflicht der Auftragsverarbeiter, mit der Aufsichtsbehörde zusammenzuarbeiten

25 / 40
Was muss unternommen werden, damit ein Verantwortlicher die Verarbeitung personenbezogener Daten an einen Auftragsverarbeiter auslagern kann?

A) Der Verantwortliche muss bei der Aufsichtsbehörde die Genehmigung einholen, die Verarbeitung der Daten auszulagern.
B) Der Verantwortliche muss die Aufsichtsbehörde fragen, ob der vereinbarte schriftliche Vertrag die Bestimmungen erfüllt.
C) Der Verantwortliche und der Auftragsverarbeiter müssen einen schriftlichen Vertrag aufsetzen und unterzeichnen, mit dem die Vertraulichkeit der Daten gewährleistet wird.
D) Der Auftragsverarbeiter muss gegenüber dem Verantwortlichen nachweisen, dass alle in der Dienstgütevereinbarung (DGV) vereinbarten Anforderungen erfüllt wurden.

26 / 40
Der Datenschutz durch Technikgestaltung, wie in Artikel 25 der Datenschutz-Grundverordnung (DSGVO) beschrieben, basiert auf sieben Grundprinzipien. Eines davon wird in der Regel als „Volle Funktionalität – Positivsumme, keine Nullsumme“ bezeichnet.

Was ist der Kernaspekt dieses Prinzips?

A) Angewandte Sicherheitsstandards müssen die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten während ihres gesamten Nutzungszeitraums gewährleisten.
B) Wenn verschiedene Arten von legitimen Zielen widersprüchlich sind, müssen die Ziele hinsichtlich des Schutzes der Privatsphäre gegenüber anderen Sicherheitszielen Vorrang haben.
C) Die Einbettung der Datenschutz in bestimmte Technologien, Prozesse oder Systeme sollte so erfolgen, dass die volle Funktionalität nicht beeinträchtigt wird.
D) Soweit möglich, sollten detaillierte Datenschutz- und Risikobewertungen durchgeführt und veröffentlicht werden, die die Datenschutzrisiken eindeutig dokumentieren.

27 / 40
Oftmals erachten Mitarbeiter, die mit personenbezogenen Daten arbeiten, Privatsphäre und Informationssicherheit als separate Angelegenheiten.

Warum ist das falsch?

A) Privatsphäre kann nicht gewährleistet werden, ohne ordnungsgemäße Informationssicherheitsmaßnahmen zu identifizieren, umzusetzen und zu überwachen.
B) Die Bestimmungen führen spezifische Maßnahmen zur Sicherstellung der Informationssicherheit an, die vor der Verarbeitung personenbezogener Daten ergriffen werden müssen.
C) Die Aufsichtsbehörde erwartet, dass die Rollen des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten integriert werden.

28 / 40
Eines der Ziele einer Datenschutz-Folgenabschätzung (DPIA) besteht darin, „das Vertrauen von Kunden und Bürgern in die Art und Weise, wie personenbezogene Daten verarbeitet werden und die Privatsphäre geachtet wird, zu stärken".

Wie kann eine DPIA „das Vertrauen stärken"?

A) Die Organisation minimiert das Risiko kostspieliger Anpassungen von Prozessen oder der Neugestaltung von Systemen zu einem späteren Zeitpunkt.
B) Die Organisation verhindert die Nichteinhaltung der Datenschutz-Grundverordnung (DSGVO) und minimiert das Risiko von Geldbußen.
C) Die Organisation weist nach, dass sie die Privatsphäre ernst nimmt und bestrebt ist, die Einhaltung der DSGVO sicherzustellen.

29 / 40
Was ist der Zweck eines Datenschutzaudits durch die Aufsichtsbehörde?

A) Die Verpflichtung der Datenschutz-Grundverordnung (DSGVO) erfüllen, geeignete technische und organisatorische Maßnahmen hinsichtlich des Datenschutzes zu implementieren.
B) Die Anwendung der DSGVO überwachen und durchsetzen, indem beurteilt wird, ob die Verarbeitung im Einklang mit der DSGVO erfolgt.
C) Den Verantwortlichen hinsichtlich der Minderung von Risiken für die Privatsphäre zu beraten, um den Verantwortlichen vor Haftungsansprüchen infolge einer Nichteinhaltung der DSGVO zu schützen.

30 / 40
Was beschreibt den Grundsatz der Datenminimierung **am besten**?

A) Es muss darauf geachtet werden, dass so wenige Daten wie möglich erhoben werden, um die Privatsphäre und Interessen der betroffenen Personen zu schützen.
B) Die Daten müssen für die Zwecke, zu denen sie verarbeitet werden, angemessen und relevant sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein.
C) Damit die Daten verwaltet werden können, müssen sie so gespeichert werden, dass so wenig Speicherplatz wie möglich benötigt wird.
D) Die Menge an Informationen, die pro betroffener Person erhoben wird, darf die von der Aufsichtsbehörde festgelegte Obergrenze nicht überschreiten.

31 / 40
Session Cookies sind die am häufigsten verwendeten Cookie-Arten.

Was macht ein Session Cookie?

A) Es enthält Informationen darüber, was Sie gerade tun, beispielsweise über die Produkte, die Sie in einem Webshop ausgewählt haben, bevor Sie Ihre Bestellung aufgeben.
B) Es zeigt Ihren Browserverlauf an, sodass andere Websites herausfinden können, welche Websites Sie zuvor besucht haben.
C) Es speichert Ihren Browserverlauf, sodass Sie nachverfolgen können, welche Seiten Sie im Internet besucht haben, und diese bei Bedarf erneut besuchen können.
D) Es erhebt Ihre personenbezogenen Daten, sodass die Website Sie mit Ihrem Namen begrüßen und Ihre Einstellungen erneut verwenden kann, wenn Sie zu ihr zurückkehren.

32 / 40
Gelegentlich sammeln Websites Informationen über Besucher und speichern diese zu Marketing-Zwecken.

Ist die Website verpflichtet, den Besucher darüber zu informieren, dass seine Informationen zu Marketing-Zwecken verwendet werden?

A) Ja
B) Nein

33 / 40
Durch die Nutzung von sozialen Medien kann sich ein Unternehmen als Experte in einem bestimmten Fachbereich präsentieren.

Was ist die **beste** Methode, um Fachwissen in einem bestimmten Bereich nachzuweisen?

A) Durch Veröffentlichung von Informationen über das Unternehmen in den sozialen Medien.
B) Durch aktive Beantwortung von Fragen zu seinem Produkt in den sozialen Medien.
C) Durch Veröffentlichungen darüber, wie minderwertig das Produkt der Konkurrenz im Vergleich zu dem Produkt Ihres Unternehmens ist.
D) Durch Veröffentlichung von Informationen über neue Produkte, die das Unternehmen entwickelt.

34 / 40
Es kam zu einer Verletzung der Sicherheit eines IT-Systems, in dem auch personenbezogene Daten gespeichert sind.

Was muss der Verantwortliche **als Erstes** tun?

A) Feststellen, ob die Verletzung zu einem Verlust oder einer unrechtmäßigen Verarbeitung personenbezogener Daten geführt hat.
B) Das Risiko nachteiliger Auswirkungen für die betroffenen Personen mittels einer Datenschutz-Folgenabschätzung (DPIA) beurteilen.
C) Beurteilen, ob möglicherweise oder tatsächlich sensible personenbezogene Daten unrechtmäßig verarbeitet wurden.
D) Die Verletzung unverzüglich der zuständigen Aufsichtsbehörde melden.

35 / 40
Das Wort „Privatsphäre“ wird in der Datenschutz-Grundverordnung (DSGVO) nicht genannt.

In welchem Zusammenhang stehen „Privatsphäre“ und „Datenschutz“?

A) Datenschutz umfasst eine Reihe von Vorschriften und Bestimmungen hinsichtlich der Verarbeitung personenbezogener Daten. Privatsphäre ist das Ergebnis des Datenschutzes.
B) Privatsphäre ist das Recht, vor der Beeinträchtigung persönlicher Angelegenheiten geschützt zu werden. Datenschutz ist das Mittel, um diesen Schutz zu gewährleisten.
C) Privatsphäre ist das Recht, persönliche Angelegenheiten geheim zu halten. Datenschutz ist das Recht, personenbezogene Daten geheim zu halten.
D) Die Begriffe „Privatsphäre“ und „Datenschutz“ sind austauschbar. Hinsichtlich der Bedeutung gibt es keinen wirklichen Unterschied.

36 / 40
Verordnung (EU) 2016/679, die als Datenschutz-Grundverordnung (DSGVO) bekannt ist, hebt eine frühere EU-Richtlinie auf.

Welche Richtlinie wird aufgehoben (ersetzt)?

A) Richtlinie 2002/58/EG vom 12. Juli 2002
B) Richtlinie 2006/24/EG vom 15. März 2006
C) Richtlinie 95/46/EG vom 24. Oktober 1995
D) Richtlinie 97/66/EG vom 15. Dezember 1997

37 / 40
Welches Recht von betroffenen Personen wird in der Datenschutz-Grundverordnung (DSGVO) ausdrücklich definiert?

A) Es muss eine Kopie der personenbezogenen Daten in dem von der betroffenen Person gewünschten Format bereitgestellt werden.
B) Kostenloser Zugriff der betroffenen Person auf personenbezogene Daten.
C) Personenbezogene Daten müssen auf Anfrage der betroffenen Person immer geändert werden.
D) Personenbezogene Daten müssen jederzeit gelöscht werden, wenn eine betroffene Person dies fordert.

38 / 40
Die Datenschutz-Grundverordnung (DSGVO) unterscheidet „sensible personenbezogene Daten“ als besondere Kategorie personenbezogener Daten.

Was ist ein Beispiel für solche Daten?

A) Ein Termin in einem Krankenhaus bei einem Facharzt
B) Eine internationale Bankkontonummer (IBAN)
C) Ein Abonnement einer politikwissenschaftlichen Zeitschrift
D) Die Mitgliedschaft in einem Branchenverband

39 / 40
Welche Rolle im Datenschutz legt den Zweck und die Mittel der Verarbeitung personenbezogener Daten fest?

A) Verantwortlicher
B) Datenschutzbeauftragter
C) Auftragsverarbeiter

40 / 40
Welche Informationen werden nach der Datenschutz-Grundverordnung (DSGVO) als personenbezogene Daten erachtet?

A) Informationen über eine Person, die die Privatsphäre dieser Person verletzen könnten, auch wenn sie falsch sind
B) Sämtliche Informationen hinsichtlich einer identifizierbaren natürlichen Person
C) Informationen hinsichtlich einer identifizierbaren natürlichen Person, die digitalisiert sind

Antwortschlüssel

1 / 40
Die rechtswidrige Erhebung, Speicherung, Änderung, Offenlegung oder Verbreitung personenbezogener Daten ist nach europäischem Recht strafbar.

Um was für eine Art von Straftat handelt es sich?

A) Eine inhaltsbezogene Straftat
B) Eine Wirtschaftsstraftat
C) Eine Straftat in Bezug auf geistiges Eigentum
D) Eine Straftat in Bezug auf die Privatsphäre

A) Falsch. Eine inhaltsbezogene Straftat betrifft die Verbreitung rassistischer Aussagen, von (Kinder-)Pornografie oder Informationen, die zu Gewalt anstiften.
B) Falsch. Wirtschaftsstraftaten betreffen den unbefugten Zugang zu Systemen (Hacking, Verbreitung von Viren usw.), Computerspionage, -fälschung und -betrug.
C) Falsch. Straftaten in Bezug auf geistiges Eigentum betreffen die Verletzung von Urheberrechten und damit verbundenen Rechten.
D) Richtig. Jede rechtswidrige Verarbeitung personenbezogener Daten ist eine Straftat. Keine Quelle: Grundkenntnisse.

2 / 40
In welchem Zusammenhang stehen Privatsphäre und Datenschutz?

A) Datenschutz ist eine Teilmenge der Privatsphäre.
B) Privatsphäre ist eine Teilmenge des Datenschutzes.
C) Die Begriffe bezeichnen dasselbe.
D) Es gibt keine Privatsphäre ohne Datenschutz.

A) Falsch. Der Begriff Privatsphäre umfasst viele Konzepte, wie z. B. räumliche, körperliche, beziehungs- und informationsbezogene Privatsphäre. Der Datenschutz steht zu einigen von diesen in keinem Bezug.
B) Falsch. Der Begriff Privatsphäre umfasst viele Konzepte, wie z. B. räumliche, körperliche, beziehungs- und informationsbezogene Privatsphäre. Datenschutz hilft dabei, einige von diesen zu gewährleisten.
C) Falsch. Datenschutz hat beispielsweise nichts mit räumlicher Privatsphäre zu tun.
D) Richtig. Datenschutz ist eine für das Grundrecht auf Schutz der der Privatsphäre erforderliche Maßnahme. Siehe: White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions.

3 / 40
Welchen **Hauptzweck** hat die Datenschutz-Grundverordnung (DSGVO)?

A) Eine gemeinsame Grundlage bilden, auf der die Mitgliedstaaten ihre eigenen Gesetze aufbauen können.
B) Nicht-EU-Länder dazu verpflichten, das Recht von Einzelpersonen aus der EU auf Privatsphäre zu achten.
C) Privatsphäre als grundlegendes Menschenrecht für alle gewährleisten.
D) Den Datenschutz für Einzelpersonen innerhalb der EU stärken und vereinheitlichen.

A) Falsch. Die DSGVO ist eine Verordnung, d. h. sie hebt die Datenschutzgesetze der einzelnen Mitgliedstaaten auf.
B) Falsch. Ihr Hauptziel ist die Festlegung von Datenschutzrechten von Einzelpersonen innerhalb der EU.
C) Falsch. Die DSGVO erklärt ausdrücklich, dass der Datenschutz ein Grundrecht ist, doch ihr Geltungsbereich ist auf Einzelpersonen innerhalb der EU beschränkt.
D) Richtig. Der Geltungsbereich der DSGVO beschränkt sich auf den Datenschutz als Recht von Einzelpersonen innerhalb der EU und zielt darauf ab, die Vorschriften innerhalb der EU zu harmonisieren. Siehe: EU-DSGVO, eine Kurzanleitung – Einführung

4 / 40
Die Datenschutz-Grundverordnung (DSGVO) bezieht sich auf den Schutz personenbezogener Daten.

Wie lautet die Definition personenbezogener Daten?

A) Alle Informationen über eine identifizierte oder identifizierbare natürliche Person
B) Alle Informationen, die europäische Bürgerinnen und Bürger schützen möchten
C) Daten, aus denen die rassische und ethnische Herkunft oder religiöse Überzeugungen direkt oder indirekt hervorgehen, sowie Daten zur Gesundheit oder zur sexuellen Orientierung
D) Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

A) Richtig. Dies ist die offizielle Definition von Datenschutz. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 2 und Artikel 4 der DSGVO 2016/679: Begriffsbestimmung.
B) Falsch. Diese Definition ist zu allgemein.
C) Falsch. Dies ist die Definition von sensiblen Daten, nicht von personenbezogenen Daten im Allgemeinen.
D) Falsch. Dies ist die Definition von Informationssicherheit nach ISO/IEC 27000:2014.

5 / 40
Welche Kategorie personenbezogener Daten wird nach der Datenschutz-Grundverordnung (DSGVO) als sensible Daten erachtet?

A) Kreditkarteninformationen
B) Sozialversicherungsnummer
C) Ausweisnummer
D) Gewerkschaftsmitgliedschaft

A) Falsch. Kreditkarteninformationen sind nach der DSGVO keine sensiblen Daten.
B) Falsch. Eine Sozialversicherungsnummer gehört nach der DSGVO nicht zu den sensiblen Daten.
C) Falsch. Ausweisinformationen sind nach der DSGVO keine sensiblen Daten.
D) Richtig. Mitgliedschaften in Gewerkschaften sind sensible Daten. Siehe: Art. 9, Erwägungsgrund 10, der DSGVO – besondere Kategorien personenbezogener Daten.

6 / 40
Wie lautet die Definition von „Verarbeitung" personenbezogener Daten nach der Datenschutz-Grundverordnung (DSGVO)?

A) Jeder Vorgang im Zusammenhang mit personenbezogenen Daten
B) Jeder Vorgang im Zusammenhang mit personenbezogenen Daten, mit Ausnahme der Löschung und Vernichtung
C) Nur Vorgänge, bei denen Daten in den sozialen Medien geteilt oder per E-Mail oder anderweitig über das Internet weitergegeben werden
D) Nur Vorgänge, bei denen personenbezogene Daten für die Zwecke verwendet werden, für die sie erhoben wurden

A) Richtig. Siehe: Art. 4(2) der DSGVO.
B) Falsch. „Verarbeitung" bezeichnet jeden Vorgang im Zusammenhang mit personenbezogenen Daten.
C) Falsch. „Verarbeitung" bezeichnet jeden Vorgang im Zusammenhang mit personenbezogenen Daten.
D) Falsch. „Verarbeitung" bezeichnet jeden Vorgang im Zusammenhang mit personenbezogenen Daten.

7 / 40
Eine unabhängige Behörde, die von einem Mitgliedstaat gemäß Artikel 51 eingerichtet wurde.

Welche Rolle im Datenschutz ist definiert?

A) Verantwortlicher
B) Auftragsverarbeiter
C) Aufsichtsbehörde
D) Dritter

A) Falsch. Siehe: Artikel 4 der DSGVO 2016/679.
B) Falsch. Siehe: Artikel 4 der DSGVO 2016/679.
C) Richtig. Siehe: Artikel 4 und Artikel 51 der DSGVO 2016/679.
D) Falsch. Siehe: Artikel 4 der DSGVO 2016/679.

8 / 40
„Informierte Einwilligung“ ist eine rechtmäßige Grundlage für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung (DSGVO). Der Zweck der Verarbeitung, für die die Einwilligung erteilt wird, muss dokumentiert werden.

Zu welchem Zeitpunkt sollte die Einwilligung der betroffenen Person eingeholt werden?

A) Nachdem die Zweckbestimmung dargelegt wurde und bevor personenbezogene Daten erhoben werden.
B) Bevor die Zweckbestimmung ausgearbeitet und dargelegt wird.
C) Bevor die personenbezogenen Daten verarbeitet werden.
D) Bevor die personenbezogenen Daten veröffentlicht oder verbreitet werden.

A) Richtig. Eine informierte Einwilligung ist nur nach Darlegung der Zweckbestimmung gegenüber der betroffenen Person möglich. Siehe: Erwägungsgründe (32), (42) der DSGVO.
B) Falsch. Eine informierte Einwilligung ist nur nach Darlegung der Zweckbestimmung gegenüber der betroffenen Person möglich.
C) Falsch. Die Erhebung personenbezogener Daten ist eine „Verarbeitung“ und bedarf daher der informierten Einwilligung der betroffenen Person.
D) Falsch. Die Veröffentlichung und Verbreitung personenbezogener Daten sind „Verarbeitungen“ und bedürfen daher der informierten Einwilligung der betroffenen Person.

9 / 40
Die Datenschutz-Grundverordnung (DSGVO) basiert auf den Grundsätzen der Verhältnismäßigkeit und der Subsidiarität.

Was bedeutet „Verhältnismäßigkeit“ in diesem Zusammenhang?

A) Personenbezogene Daten können nur entsprechend der Zweckbestimmung verarbeitet werden.
B) Personenbezogene Daten können ohne ausdrückliche und informierte Einwilligung nicht wiederverwendet werden.
C) Personenbezogene Daten dürfen nur verarbeitet werden, wenn es keine anderen Mittel gibt, um die Zwecke zu erreichen.
D) Personenbezogene Daten müssen in Bezug auf die Zwecke angemessen und relevant sein und sich im Rahmen halten.

A) Falsch. Dies ist eine der gesetzlichen Einschränkungen.
B) Falsch. Dies ist eine der gesetzlichen Einschränkungen.
C) Falsch. Dies ist die Definition von Subsidiarität.
D) Richtig. Siehe: White Paper – Privacy, Personal Data and the GDPR - §3.1.2 Proportionality and subsidiarity und Art. 35 (7) der DSGVO.

10 / 40
Die Verarbeitung personenbezogener Daten muss den allgemeinen Qualitätsvorschriften entsprechen.

Was ist eine der in der Datenschutz-Grundverordnung (DSGVO) definierten Vorschriften?

A) Die verarbeiteten Daten müssen archiviert werden.
B) Die verarbeiteten Daten müssen verschlüsselt werden.
C) Die verarbeiteten Daten müssen indiziert werden.
D) Die verarbeiteten Daten müssen relevant sein.

A) Falsch In der DSGVO ist keine solche Anforderung definiert.
B) Falsch. In der DSGVO ist keine solche Anforderung definiert.
C) Falsch. In der DSGVO ist keine solche Anforderung definiert.
D) Richtig. Diese Anforderung ist in der DSGVO definiert. Siehe: White Paper – Privacy, Personal Data and the GDPR - §3.1.2 Proportionality and subsidiarity

11 / 40
Jedes Mal, wenn personenbezogene Daten verarbeitet werden, müssen Verhältnismäßigkeit und Subsidiarität geprüft werden.

Was ist eine Anforderung an die Verarbeitung personenbezogener Daten?

A) Sie muss von der kleinstmöglichen Anzahl von Mitarbeitern vorgenommen werden, die für den Verantwortlichen oder ein verbundenes Unternehmen arbeiten.
B) Sie muss immer auf das für die Zielerreichung Notwendige, und auf die am wenigsten „in die Privatsphäre eingreifenden" Daten beschränkt sein.
C) Sie muss auf eine vordefinierte Speichergröße beschränkt sein, und das verwendete System muss von dem Verantwortlichen finanziert werden.
D) Sie muss für die kleinstmögliche Anzahl von Zwecken verwendet werden und darf nicht außerhalb der Räumlichkeiten des Auftragsverarbeiters erfolgen.

A) Falsch. Die Anzahl der Mitarbeiter oder deren Zugehörigkeit zu einer Tochtergesellschaft hat nichts mit diesen Bestimmungen zu tun.
B) Richtig. Diese Bestimmungen bedeuten, dass Sie ausschließlich jene Daten erfassen, die erforderlich sind, um das bzw. die vordefinierte(n) Ziel(e) zu erreichen, und stets versuchen, Daten zu verwenden, die die geringsten Auswirkungen auf die Privatsphäre der betreffenden Person haben. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3
C) Falsch. Die Speichergröße und wer die verwendeten Systeme finanziert, hat nichts mit diesen Bestimmungen zu tun.
D) Falsch. Solange die betroffene Person ihre Einwilligung erteilt hat, gibt es keine expliziten Beschränkungen hinsichtlich der Anzahl der Ziele oder des Standorts.

12 / 40
Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass (...) nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck der Verarbeitung erforderlich sind.

Welcher Begriff ist in der Datenschutz-Grundverordnung (DSGVO) definiert?

A) Einhaltung
B) Datenschutz durch datenschutzfreundliche Voreinstellungen
C) Datenschutz durch Technikgestaltung
D) Eingebetteter Schutz

A) Falsch. Der Begriff Einhaltung bezeichnet den Zustand oder die Tatsache der Erfüllung oder Befolgung von Vorschriften oder Standards.
B) Richtig. Mit datenschutzfreundlichen Voreinstellungen ist das Minimum an personenbezogenen Daten für den kürzest möglichen Zeitraum zu verarbeiten, wobei die bestmöglichen Sicherheitsmaßnahmen zur Verhinderung eines unbefugten Zugriffs zu verwenden sind. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Art. 20 (2) der DSGVO.
C) Falsch. Datenschutz durch Technikgestaltung bezieht sich auf eine Technikgestaltung, die geeignete Maßnahmen zur Umsetzung der Datenschutzgrundsätze beinhaltet.
D) Falsch. Eingebetteter Datenschutz ist das Ergebnis von Datenschutz durch Technikgestaltung.

13 / 40
Wie lautet der Begriff für die unbefugte Weitergabe von oder den unbefugten Zugriff auf personenbezogene(n) Daten in der Datenschutz-Grundverordnung (DSGVO)?

A) Verletzung der Geheimhaltungspflicht
B) Verletzung des Schutzes personenbezogener Daten
C) Zwischenfall
D) Sicherheitsvorfall

A) Falsch. Die DSGVO verwendet den Begriff Verletzung des Schutzes personenbezogener Daten. Nicht jede Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Geheimhaltungspflicht.
B) Richtig. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Artikel 4 (12) der DSGVO
C) Falsch. Die DSGVO verwendet den Begriff Verletzung des Schutzes personenbezogener Daten. Nicht jeder Zwischenfall ist eine Verletzung des Schutzes personenbezogener Daten.
D) Falsch. Die DSGVO verwendet den Begriff Verletzung des Schutzes personenbezogener Daten. Nicht jeder Sicherheitsvorfall ist eine Verletzung des Schutzes personenbezogener Daten.

14 / 40
Es wurde festgestellt, dass es zu einer Verletzung des Schutzes sensibler personenbezogener Daten gekommen ist.

Wem muss diese Verletzung letztendlich nach der Datenschutz-Grundverordnung (DSGVO) gemeldet werden?

A) Dem Datenschutzbeauftragten
B) Der Aufsichtsbehörde
C) Dem Abteilungsleiter
D) Der Polizei

A) Falsch. Auch wenn die Verletzung einem internen Datenschutzbeauftragten gemeldet werden kann, muss sie letztendlich der Aufsichtsbehörde gemeldet werden.
B) Richtig. Verletzungen des Schutzes personenbezogener Daten müssen der Aufsichtsbehörde gemeldet werden, wenn sie erhebliche Folgen für die Sicherheit der betroffenen Person oder deren personenbezogener Daten haben könnten. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Artikel 4 (12) der DSGVO
C) Falsch. Auch wenn die Verletzung dem Vorgesetzten gemeldet werden kann, muss sie letztendlich der Aufsichtsbehörde gemeldet werden.
D) Falsch. Verletzungen des Schutzes personenbezogener Daten müssen nicht unbedingt der Polizei gemeldet werden, doch letztendlich müssen sie der Aufsichtsbehörde gemeldet werden.

15 / 40
Bei der Erstellung einer Sicherungskopie stürzt eine Server-Festplatte ab. Sowohl die Daten als auch die Sicherungskopie gehen verloren. Die Festplatte enthielt personenbezogene Daten, aber keine sensiblen Daten.

Um was für einen Zwischenfall handelt es sich?

A) Verletzung des Schutzes personenbezogener Daten
B) Verletzung der Sicherheit
C) Sicherheitsvorfall

A) Richtig. Personenbezogene Daten, die unwiederbringlich verloren gegangen sind, gelten als unbefugte Verarbeitung, was eine Verletzung des Schutzes personenbezogener Daten darstellt. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3, und Kapitel I, Artikel 4 der DSGVO: Begriffsbestimmungen.
B) Falsch. Personenbezogene Daten, die unwiederbringlich verloren gegangen sind, gelten als unbefugte Verarbeitung, was eine Verletzung des Schutzes personenbezogener Daten darstellt.
C) Falsch. Personenbezogene Daten, die unwiederbringlich verloren gegangen sind, gelten als unbefugte Verarbeitung, was eine Verletzung des Schutzes personenbezogener Daten darstellt.

16 / 40
Eine Person, die für eine Gewerkschaft arbeitet, hat einen Newsletter-Entwurf mit nach Hause genommen, um ihn dort für die Mitglieder fertigzustellen. Der USB-Stick mit dem Entwurf und der Mailingliste ist verloren gegangen.

Wem muss diese Verletzung des Schutzes personenbezogener Daten neben der Datenschutzbehörde noch gemeldet werden?

A) Allen Mitgliedern auf der Mailingliste
B) Den Gewerkschaftsmitarbeitern
C) Der Polizei

A) Richtig. Dies sind sensible Daten. Daher muss der Verlust sowohl der Datenschutzbehörde als auch den betroffenen Personen gemeldet werden: EU-DSGVO, eine Kurzanleitung – Kapitel 3 Die Verordnung – Datenverletzungen.
B) Falsch. Dies sind sensible Daten, daher muss der Verlust sowohl der Datenschutzbehörde als auch den betroffenen Personen gemeldet werden.
C) Falsch. Dies sind sensible Daten, daher muss der Verlust sowohl der Datenschutzbehörde als auch den betroffenen Personen gemeldet werden.

17 / 40
Eine Organisation für Sozialdienste plant, eine neue Datenbank zu entwickeln, um ihre Kunden und deren Pflegebedarf zu verwalten.

Worin besteht einer der ersten wichtigen Schritte, um eine Genehmigung der Aufsichtsbehörde zu beantragen?

A) Daten über die Kunden und die Menge und Art der benötigten und erbrachten Pflegeleistungen erheben.
B) Eine Datenschutz-Folgenabschätzung (DPIA) zur Bewertung der Risiken der beabsichtigten Verarbeitung durchführen.
C) Die Einwilligung der Kunden für die beabsichtigte Verarbeitung ihrer personenbezogenen Daten einholen.

A) Falsch. Die Erhebung medizinischer personenbezogener Daten ist per Definition die „Verarbeitung sensibler Daten“. Es ist die vorherige Genehmigung der Aufsichtsbehörde und der betroffenen Person erforderlich.
B) Richtig. Bei der Einholung der Einwilligung zur Datenverarbeitung muss die betroffene Person „über Risiken, Vorschriften, Garantien und Rechte informiert werden ...“. Es ist eine DPIA erforderlich, um diese Risiken und Garantien zu beurteilen. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Erwägungsgrund (39) der DSGVO.
C) Falsch. Bei der Einholung der Einwilligung zur Datenverarbeitung muss die betroffene Person „über Risiken, Vorschriften, Garantien und Rechte informiert werden ...“. Es ist zunächst eine DPIA erforderlich, um diese Risiken und Garantien zu beurteilen.

18 / 40
In welchem Fall müssen die betroffenen Personen immer über eine Verletzung des Schutzes personenbezogener Daten informiert werden?

A) Die personenbezogenen Daten wurden in einer Einrichtung des Auftragsverarbeiters verarbeitet, die sich außerhalb der EU befindet..
B) Die personenbezogenen Daten wurden von einer Partei verarbeitet, die zwar dem Entwurf des vom Verantwortlichen vorgelegten Vertrags zur Auftragsverarbeitung zugestimmt, diesen aber noch nicht verbindlich unterzeichnet hat.
C) Das System, auf dem die personenbezogenen Daten verarbeitet wurden, wurde angegriffen und die Speichermedien des Systems wurden bei dem Angriff beschädigt.
D) Es besteht eine große Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten sich nachteilig auf den Schutz der Privatsphäre der betroffenen Personen auswikrt.

A) Falsch. Der Ort, an dem die Daten verarbeitet werden, ist für die Pflicht zur Benachrichtigung der betroffenen Personen über die Verletzungen des Schutzes personenbezogener Daten nicht von Bedeutung.
B) Falsch. Die Verarbeitung personenbezogener Daten von einer anderen Partei als dem Verantwortlichen, ohne dass ein verbindlicher Vertrag besteht, gilt als Verletzung des Schutzes personenbezogener Daten. In dem hier vorliegenden Fall jedoch sind negative Auswirkungen für die betroffenen Personen unwahrscheinlich. Die Information der betroffenen Personen ist daher nicht obligatorisch.
C) Falsch. Schäden an Speichermedien machen den Zugriff auf Daten schwierig oder sogar unmöglich, implizieren aber keine rechtswidrige Verarbeitung.
D) Richtig. Sind nachteilige Auswirkungen auf die betroffenen Personen wahrscheinlich, so ist der Verantwortliche verpflichtet, die betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten in Kenntnis zu setzen. Quelle: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs

19 / 40
Ein niederländischer Verantwortlicher hat die Verarbeitung sensibler personenbezogener Daten an einen Auftragsverarbeiter in einem nordafrikanischen Land vergeben, ohne die Aufsichtsbehörde zu konsultieren. Dies wurde aufgedeckt und von der Aufsichtsbehörde bestraft.

Sechs Monate später stellt die Aufsichtsbehörde fest, dass sich der Verantwortliche des gleichen Verstoßes bei einem anderen Verarbeitungsvorgang schuldig gemacht hat.

Was ist das maximale Bußgeld, das die Aufsichtsbehörde in diesem Fall verhängen kann?

A) € 750.000
B) € 1.230.000
C) € 10.000.000 oder 2 % des weltweiten Umsatzes des Unternehmens, je nachdem, was höher ist
D) € 20.000.000 oder 4 % des weltweiten Umsatzes des Unternehmens, je nachdem, was höher ist

A) Falsch. Nach Art. 83.3 der Datenschutz-Grundverordnung (DSGVO) ist das maximale Bußgeld € 20.000.000 oder 4% des weltweiten Umsatzes des Unternehmens, je nachdem was höher ist.
B) Falsch. Nach Art. 83.3 der DSGVO ist das maximale Bußgeld € 20.000.000 oder 4% des weltweiten Umsatzes des Unternehmens, je nachdem was höher ist.
C) Falsch. Nach Art. 83.3 der DSGVO ist das maximale Bußgeld € 20.000.000 oder 4% des weltweiten Umsatzes des Unternehmens, je nachdem was höher ist.
D) Richtig. Nach Art. 83.3 der DSGVO, sind solche Rechtsverletzungen Gegenstand von Bußgeldforderungen in der Höhe von maximal € 20.000.000 oder im Falle eines Wirtschaftsunternehmens, bis zu 4 % des weltweiten Jahresumsatzes basierend auf dem Umsatz des vorhergehenden Geschäftsjahres, je nachdem, was höher ist. Sieher: White Paper – Privacy, Personal Data and the GDPR - §7.3.3 General conditions for imposing administrative fines.

.

20 / 40
Den Aufsichtsbehörden ist eine Reihe von Pflichten auferlegt, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten.

Was ist eine dieser Pflichten?

A) Beurteilung von Verhaltenskodizes für bestimmte Sektoren in Bezug auf die Verarbeitung personenbezogener Daten.
B) Festlegung eines Mindestmaßes von Maßnahmen zum Schutz personenbezogener Daten.
C) Untersuchung aller Verletzungen des Schutzes personenbezogener Daten, die ihnen gemeldet wurden.
D) Überprüfung der Verträge und verbindlichen internen Datenschutzvorschriften auf die Einhaltung der Bestimmungen.

A) Richtig. Eine der Pflichten der Aufsichtsbehörden besteht darin, allgemeine Ratschläge zur Einhaltung der Vorschriften zu geben. Siehe: White Paper – Privacy, Personal Data and the GDPR - §7.1.4 To set standards.
B) Falsch. Eine Aufsichtsbehörde gibt allgemeine Ratschläge dazu, was sie als geeignetes Maß an Sicherheit erachtet. Sie wird Ihnen jedoch nicht erklären, welche konkreten Maßnahmen Sie ergreifen müssen, um dieses Maß an Sicherheit zu erreichen. Auch wenn sie es gerne würde, ist sie nicht in der Lage dazu, da es einfach keine Einheitslösung gibt.
C) Falsch. Aufsichtsbehörden sind weder verpflichtet noch verfügen sie über die Kapazität, alle Verletzungen zu untersuchen, von denen sie Kenntnis erlangen. Doch sie werden diejenigen untersuchen, die sie für bedeutsam oder bemerkenswert halten.
D) Falsch. Aufsichtsbehörden bieten keine Rechtsberatung. Sie überprüfen keine Verträge und keine verbindlichen internen Datenschutzvorschriften. Im Rahmen einer Untersuchung können sie sich jedoch einen bestimmten Vertrag oder verbindliche interne Datenschutzvorschriften näher ansehen.

21 / 40
Eine religiöse Vereinigung möchte personenbezogene Daten an ihre religiöse Autorität in einem außereuropäischen Land weitergeben, um eine rechtliche Anforderung der betreffenden Regierung einzuhalten.

Welche Bestimmung der Datenschutz-Grundverordnung (DSGVO) gilt in diesem Fall?

A) Als Ausnahmeregelung ist einer religiösen Vereinigung die Verarbeitung sensibler Daten, aus denen religiöse Überzeugungen hervorgehen, gestattet.
B) Es ist rechtlich nicht zulässig, personenbezogene Daten aus der EU als Reaktion auf eine rechtliche Anforderung eines Drittlandes zu übermitteln.
C) Die Verarbeitung ist rechtlich zulässig, sofern eine spezifische und eindeutige Einwilligung der betroffenen Person eingeholt wurde.
D) Die Verarbeitung personenbezogener Daten außerhalb der EU ist nach den von der EU-Kommission ausgearbeiteten Standartvertragsklauseln zulässig.

A) Falsch. Religiöse Vereinigungen sind berechtigt, personenbezogene Daten über ihre früheren und derzeitigen Mitglieder zu verarbeiten, es ist ihnen jedoch nicht erlaubt, personenbezogene Daten aus der EU als Reaktion auf eine rechtliche Anforderung eines Drittlandes zu übermitteln.
B) Richtig. Siehe: White Paper – Privacy, Personal Data and the GDPR - §7.5.2 Regulations applying to data transfer outside the EEA, EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Art. 48 der DSGVO.
C) Falsch. Es ist rechtlich nicht zulässig, personenbezogene Daten aus der EU als Reaktion auf eine rechtliche Anforderung eines Drittlandes zu übermitteln, auch nicht mit der Einwilligung der betroffenen Person.
D) Falsch. Die Verarbeitung sensibler Daten außerhalb der EU kann rechtlich zulässig sein, aber nicht als Reaktion auf den Antrag einer Regierung eines Drittlandes.

22 / 40
Am 12. Juli 2016 hat die Europäische Kommission eine Entscheidung über die Übermittlung personenbezogener Daten mit den USA (EU-US-Datenschutzschild) umgesetzt.

Welche Art von Entscheidung ist dies im Sinne der Datenschutz-Grundverordnung (DSGVO)?

A) Ein Angemessenheitsbeschluss
B) Ein Ausnahmeerlass
C) Ein verbindlicher Standardvertrag
D) Ein die DSGVO ersetzendes Abkommen

A) Richtig. Die Entscheidung ist ein Angemessenheitsbeschluss im Einklang mit der DSGVO in Bezug auf die Verarbeitung in Drittländern. Siehe: White Paper – Privacy, Personal Data and the GDPR - §7.5.4 Regulations applying to data transfer between the EEA and the USA, EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Erwägungsgründe 104 und 106 der DSGVO.
B) Falsch. Eine Ausnahme sind Übermittlungen, die unerlässlich sind, um auf terroristische Straftaten oder schwere Verbrechen reagieren zu können (Art. 11)
C) Falsch. Die Entscheidung ist ein Angemessenheitsbeschluss im Einklang mit der DSGVO in Bezug auf die Verarbeitung in Drittländern.
D) Falsch. Die Entscheidung ist ein Angemessenheitsbeschluss im Einklang mit der DSGVO in Bezug auf die Verarbeitung in Drittländern.

23 / 40
Verbindliche interne Datenschutzvorschriften dienen Organisationen als Mittel, um ihren administrativen Aufwand hinsichtlich der Einhaltung der Datenschutz-Grundverordnung (DSGVO) zu reduzieren.

Inwiefern helfen ihnen diese Vorschriften?

A) Sie ermöglichen ihnen, unterstützende Verträge mit allen Beteiligten im Ausland abzuschließen.
B) Sie ermöglichen ihnen, personenbezogene Daten durch Dritte außerhalb des Europäischen Wirtschaftsraums (EWR) verarbeiten zu lassen.
C) Sie vermeiden die Notwendigkeit, jede Aufsichtsbehörde in dem EWR einzeln informieren zu müssen.
D) Sie verhindern, dass sie von einer Aufsichtsbehörde die Genehmigung zur Verarbeitung der Daten einholen müssen, sobald ihre verbindlichen internen Datenschutzvorschriften akzeptiert wurden.

A) Falsch. Verbindliche interne Datenschutzvorschriften werden erarbeitet, damit Organisationen nicht für jedes verbundene Unternehmen separate schriftliche unterstützende Verträge verwenden müssen.
B) Falsch. Verbindliche interne Datenschutzvorschriften sind innerhalb einer Organisation und aller ihrer verbundenen Unternehmen gültig. Sie gelten nicht für andere Parteien.
C) Richtig. Sobald verbindliche interne Datenschutzvorschriften von einer Aufsichtsbehörde innerhalb des EWRs genehmigt wurden, müssen Sie von den anderen Aufsichtsbehörden innerhalb des EWRs keine Genehmigung mehr einholen. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3.
D) Falsch. Verbindliche interne Datenschutzvorschriften müssen auch von einer Aufsichtsbehörde genehmigt werden.

24 / 40
Falls ein Auftragnehmer die Verarbeitung personenbezogener Daten an eine andere Partei abgibt, schließen die Parteien einen schriftlichen Vertrag. Dieser Vertrag legt den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen fest.

Welcher andere Aspekt muss durch diesen schriftlichen Vertrag geregelt werden?

A) Die Rechenschaftspflicht des Auftragsverarbeiters
B) Die Meldepflicht im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten
C) Die Pflichten und Rechte des Verantwortlichen
D) Die Pflicht der Auftragsverarbeiter, mit der Aufsichtsbehörde zusammenzuarbeiten

A) Falsch. Dies ist eine direkte Pflicht, die die Datenschutz-Grundverordnung (DSGVO) Auftragsverarbeitern auferlegt.
B) Falsch. Dies ist eine direkte Pflicht, die die DSGVO Auftragsverarbeitern auferlegt.
C) Richtig. Dies ist eine direkte Pflicht, die die DSGVO Auftragsverarbeitern auferlegt. Siehe: EU-DSGVO, eine Kurzanlage – Kapitel 3 und Art. 22 (3) der DSGVO.
D) Falsch. Dies ist eine direkte Pflicht, die die DSGVO Auftragsverarbeitern auferlegt.

25 / 40
Was muss unternommen werden, damit ein Verantwortlicher die Verarbeitung personenbezogener Daten an einen Auftragsverarbeiter auslagern kann?

A) Der Verantwortliche muss bei der Aufsichtsbehörde die Genehmigung einholen, die Verarbeitung der Daten auszulagern.
B) Der Verantwortliche muss die Aufsichtsbehörde fragen, ob der vereinbarte schriftliche Vertrag die Bestimmungen erfüllt.
C) Der Verantwortliche und der Auftragsverarbeiter müssen einen schriftlichen Vertrag aufsetzen und unterzeichnen, mit dem die Vertraulichkeit der Daten gewährleistet wird.
D) Der Auftragsverarbeiter muss gegenüber dem Verantwortlichen nachweisen, dass alle in der Dienstgütevereinbarung (DGV) vereinbarten Anforderungen erfüllt wurden.

A) Falsch. Sie müssen nicht bei jedem Fall von Outsourcing eine Genehmigung der Aufsichtsbehörde einholen.
B) Falsch. Die Aufsichtsbehörde bietet keine Rechtsberatung und prüft keine Verträge auf Einhaltung der Bestimmungen.
C) Richtig. Es muss ein schriftlicher Vertrag bestehen, der die Vertraulichkeit der Daten gewährleistet und in dem der Verantwortliche die Ziele und Mittel der Verarbeitung festlegt. Beide Parteien müssen diesen Vertrag unterzeichnen. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3 und Art. 22 (3) der DSGVO.
D) Falsch. Eine DGV ist nicht ausreichend, da sie sich auf Vorgänge konzentriert, und nicht unbedingt auf das Festlegen von Zielen.

26 / 40
Der Datenschutz durch Technikgestaltung, wie in Artikel 25 der Datenschutz-Grundverordnung (DSGVO) beschrieben, basiert auf sieben Grundprinzipien. Eines davon wird in der Regel als „Volle Funktionalität – Positivsumme, keine Nullsumme“ bezeichnet.

Was ist der Kernaspekt dieses Prinzips?

A) Angewandte Sicherheitsstandards müssen die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten während ihres gesamten Nutzungszeitraums gewährleisten.
B) Wenn verschiedene Arten von legitimen Zielen widersprüchlich sind, müssen die Ziele hinsichtlich des Schutzes der Privatsphäre gegenüber anderen Sicherheitszielen Vorrang haben.
C) Die Einbettung der Datenschutz in bestimmte Technologien, Prozesse oder Systeme sollte so erfolgen, dass die volle Funktionalität nicht beeinträchtigt wird.
D) Soweit möglich, sollten detaillierte Datenschutz- und Risikobewertungen durchgeführt und veröffentlicht werden, die die Datenschutzrisiken eindeutig dokumentieren.

A) Falsch. Dies ist ein Aspekt der „Durchgängigen Sicherheit – Schutz der Privatsphäre über den gesamten Nutzungszeitraum“, eines der anderen sechs Grundprinzipien.
B) Falsch. Datenschutz durch Technikgestaltung lehnt den Ansatz ab, dass Privatsphäre mit anderen legitimen Interessen, Technikzielen und technischen Kapazitäten konkurrieren muss. Alle Objekte müssen im Sinne einer Positivsumme aufgenommen werden, die ein zufriedenstellendes Ergebnis für beide Seiten erzielt.
C) Richtig, das ist der Kernaspekt. Siehe: White Paper – Privacy, Personal Data and the GDPR - §8.1.1 The seven principles of data protection by design und Art. 25 der DSGVO.
D) Falsch. Dies ist ein Aspekt des „in die Technikgestaltung eingebetteten Schutzes der Privatsphäre“, eines der anderen sechs Grundprinzipien.

27 / 40
Oftmals erachten Mitarbeiter, die mit personenbezogenen Daten arbeiten, Privatsphäre und Informationssicherheit als separate Angelegenheiten.

Warum ist das falsch?

A) Privatsphäre kann nicht gewährleistet werden, ohne ordnungsgemäße Informationssicherheitsmaßnahmen zu identifizieren, umzusetzen und zu überwachen.
B) Die Bestimmungen führen spezifische Maßnahmen zur Sicherstellung der Informationssicherheit an, die vor der Verarbeitung personenbezogener Daten ergriffen werden müssen.
C) Die Aufsichtsbehörde erwartet, dass die Rollen des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten integriert werden.

A) Richtig. Privatsphäre und Datenschutz gewährleisten u. a. die Vertraulichkeit personenbezogener Daten. Dies erfordert die Umsetzung von Sicherheitsmaßnahmen. Siehe: White Paper – Privacy, Personal Data and the GDPR - §2.1.6 - integrity and confidentiality.
B) Falsch. Die Bestimmungen geben Ziele vor, die erfüllt werden müssen. Es müssen jedoch keine spezifischen Maßnahmen ergriffen werden.
C) Falsch. Die Aufsichtsbehörde erwartet nicht, dass diese Rollen integriert werden.

28 / 40
Eines der Ziele einer Datenschutz-Folgenabschätzung (DPIA) besteht darin, „das Vertrauen von Kunden und Bürgern in die Art und Weise, wie personenbezogene Daten verarbeitet werden und die Privatsphäre geachtet wird, zu stärken“.

Wie kann eine DPIA „das Vertrauen stärken“?

A) Die Organisation minimiert das Risiko kostspieliger Anpassungen von Prozessen oder der Neugestaltung von Systemen zu einem späteren Zeitpunkt.
B) Die Organisation verhindert die Nichteinhaltung der Datenschutz-Grundverordnung (DSGVO) und minimiert das Risiko von Geldbußen.
C) Die Organisation weist nach, dass sie die Privatsphäre ernst nimmt und bestrebt ist, die Einhaltung der DSGVO sicherzustellen.

A) Falsch. Dieser Aspekt mag zwar das Vertrauen des Managements stärken, aber nicht der Kunden oder Bürger.
B) Falsch. Die Vermeidung von Geldbußen mag zwar das Vertrauen des Managements stärken, aber nicht der Kunden oder Bürger.
C) Richtig. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3.

29 / 40
Was ist der Zweck eines Datenschutzaudits durch die Aufsichtsbehörde?

A) Die Verpflichtung der Datenschutz-Grundverordnung (DSGVO) erfüllen, geeignete technische und organisatorische Maßnahmen hinsichtlich des Datenschutzes zu implementieren.
B) Die Anwendung der DSGVO überwachen und durchsetzen, indem beurteilt wird, ob die Verarbeitung im Einklang mit der DSGVO erfolgt.
C) Den Verantwortlichen hinsichtlich der Minderung von Risiken für die Privatsphäre zu beraten, um den Verantwortlichen vor Haftungsansprüchen infolge einer Nichteinhaltung der DSGVO zu schützen.

A) Falsch. Das Audit ist nicht die Umsetzung der Maßnahmen, sondern eine Beurteilung deren Wirksamkeit.
B) Richtig. Laut Art. 57.1(a) der DSGVO ist dies eine wichtige Aufgabe der DSB als Aufsichtsbehörde.
C) Falsch. Die Aufsichtsbehörde hat die Aufgabe, die Einhaltung der DSGVO zu überwachen und hinsichtlich Verbesserungen zu beraten. Ihr Zweck besteht jedoch nicht darin, den Verantwortlichen zu schützen.

30 / 40
Was beschreibt den Grundsatz der Datenminimierung **am besten**?

A) Es muss darauf geachtet werden, dass so wenige Daten wie möglich erhoben werden, um die Privatsphäre und Interessen der betroffenen Personen zu schützen.
B) Die Daten müssen für die Zwecke, zu denen sie verarbeitet werden, angemessen und relevant sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein.
C) Damit die Daten verwaltet werden können, müssen sie so gespeichert werden, dass so wenig Speicherplatz wie möglich benötigt wird.
D) Die Menge an Informationen, die pro betroffener Person erhoben wird, darf die von der Aufsichtsbehörde festgelegte Obergrenze nicht überschreiten.

A) Falsch. In der Tat legt die Datenschutz-Grundverordnung (DSGVO) fest, dass die erhobenen Daten angemessen sein müssen, was bedeutet, dass nicht möglichst wenige Daten erhoben werden müssen.
B) Richtig. Dies ist die genaue Definition von Datenminimierung (Artikel 5.1.c). Mit ihr soll sichergestellt werden, dass nur Daten erhoben werden, die zur Erreichung der festgelegten Ziele erforderlich sind. Siehe: White Paper – Privacy, Personal Data and the GDPR - §2.1 Data processing principles und Art. 5.1.c der DSGVO.
C) Falsch. Die Speichergröße steht mit diesem Grundsatz nicht im Zusammenhang.
D) Falsch. Aufsichtsbehörden setzen keine Obergrenze für die Menge an erhobenen Informationen fest, solange diese erforderlich sind, um die festgelegten Ziele zu erreichen.

31 / 40
Session Cookies sind die am häufigsten verwendeten Cookie-Arten.

Was macht ein Session Cookie?

A) Es enthält Informationen darüber, was Sie gerade tun, beispielsweise über die Produkte, die Sie in einem Webshop ausgewählt haben, bevor Sie Ihre Bestellung aufgeben.
B) Es zeigt Ihren Browserverlauf an, sodass andere Websites herausfinden können, welche Websites Sie zuvor besucht haben.
C) Es speichert Ihren Browserverlauf, sodass Sie nachverfolgen können, welche Seiten Sie im Internet besucht haben, und diese bei Bedarf erneut besuchen können.
D) Es erhebt Ihre personenbezogenen Daten, sodass die Website Sie mit Ihrem Namen begrüßen und Ihre Einstellungen erneut verwenden kann, wenn Sie zu ihr zurückkehren.

A) Richtig. Ein Session Cookie wird gespeichert, um Informationen zur Sitzung zu speichern. Wenn Sie die Sitzung beenden, wird es gelöscht. Siehe: White Paper – Privacy, Personal Data and the GDPR - §8.6.3 Cookies
B) Falsch. Ein Session Cookie wird gelöscht, wenn Sie eine Sitzung beenden, sodass es bei der nächsten Sitzung nicht verwendet werden kann.
C) Falsch. Ein Session Cookie wird gelöscht, wenn Sie eine Sitzung beenden, sodass es bei der nächsten Sitzung nicht verwendet werden kann.
D) Falsch. Ein Session Cookie wird gelöscht, wenn Sie eine Sitzung beenden, sodass es bei der nächsten Sitzung nicht verwendet werden kann.

32 / 40
Gelegentlich sammeln Websites Informationen über Besucher und speichern diese zu Marketing-Zwecken.

Ist die Website verpflichtet, den Besucher darüber zu informieren, dass seine Informationen zu Marketing-Zwecken verwendet werden?

A) Ja
B) Nein

A) Richtig. Die Website ist verpflichtet, den Besucher darüber zu informieren, dass seine Informationen zu Marketing-Zwecken verwendet werden. Er hat das Recht, der Verarbeitung seiner personenbezogenen Daten zu Marketing-Zwecken zu widersprechen. Siehe: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Falsch. Die Website ist verpflichtet, den Besucher darüber zu informieren, dass seine Informationen zu Marketing-Zwecken verwendet werden. Er hat das Recht, der Verarbeitung seiner personenbezogenen Daten zu Marketing-Zwecken zu widersprechen.

33 / 40
Durch die Nutzung von sozialen Medien kann sich ein Unternehmen als Experte in einem bestimmten Fachbereich präsentieren.

Was ist die **beste** Methode, um Fachwissen in einem bestimmten Bereich nachzuweisen?

A) Durch Veröffentlichung von Informationen über das Unternehmen in den sozialen Medien.
B) Durch aktive Beantwortung von Fragen zu seinem Produkt in den sozialen Medien.
C) Durch Veröffentlichungen darüber, wie minderwertig das Produkt der Konkurrenz im Vergleich zu dem Produkt Ihres Unternehmens ist.
D) Durch Veröffentlichung von Informationen über neue Produkte, die das Unternehmen entwickelt.

A) Falsch. Wenn Sie lediglich Informationen über das Unternehmen veröffentlichen, macht Sie dies nicht zu einem Experten in einem bestimmten Bereich.
B) Richtig. Das Beantworten (und aktive Beantworten) von Fragen zu einem bestimmten Produkt in den sozialen Medien könnte Ihr Unternehmen zu einem Experten machen. Siehe: White Paper – Privacy, Personal Data and the GDPR - § 8.6 Practice related applications of the use of data, marketing and social media.
C) Falsch. Sie geben lediglich damit an, wie gut Ihr Produkt ist (was es in Wirklichkeit vielleicht gar nicht ist).
D) Falsch. Dies zeigt nur, dass Ihr Unternehmen neue Produkte entwickelt. Es könnte zwar in der Tat dabei helfen, den Umsatz zu steigern, aber macht das Unternehmen zu keinem Experten.

34 / 40
Es kam zu einer Verletzung der Sicherheit eines IT-Systems, in dem auch personenbezogene Daten gespeichert sind.

Was muss der Verantwortliche **als Erstes** tun?

A) Feststellen, ob die Verletzung zu einem Verlust oder einer unrechtmäßigen Verarbeitung personenbezogener Daten geführt hat.
B) Das Risiko nachteiliger Auswirkungen für die betroffenen Personen mittels einer Datenschutz-Folgenabschätzung (DPIA) beurteilen.
C) Beurteilen, ob möglicherweise oder tatsächlich sensible personenbezogene Daten unrechtmäßig verarbeitet wurden.
D) Die Verletzung unverzüglich der zuständigen Aufsichtsbehörde melden.

A) Richtig. Die Meldepflicht im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten gemäß dem niederländischen Datenschutzgesetz. Siehe: White Paper – Privacy, Personal Data and the GDPR - §5.2 Procedures on how to act when a data breach occurs.
B) Falsch. Eine DPIA wird bei der Entwicklung von Verarbeitungsvorgängen personenbezogener Daten durchgeführt.
C) Falsch. Der Verantwortliche muss zunächst feststellen, ob der Zwischenfall eine Verletzung des Schutzes personenbezogener Daten darstellt, die gemeldet werden muss.
D) Falsch. Der Verantwortliche muss zunächst feststellen, ob der Zwischenfall eine Verletzung des Schutzes personenbezogener Daten darstellt, die gemeldet werden muss.

35 / 40
Das Wort „Privatsphäre“ wird in der Datenschutz-Grundverordnung (DSGVO) nicht genannt.

In welchem Zusammenhang stehen „Privatsphäre“ und „Datenschutz“?

A) Datenschutz umfasst eine Reihe von Vorschriften und Bestimmungen hinsichtlich der Verarbeitung personenbezogener Daten. Privatsphäre ist das Ergebnis des Datenschutzes.
B) Privatsphäre ist das Recht, vor der Beeinträchtigung persönlicher Angelegenheiten geschützt zu werden. Datenschutz ist das Mittel, um diesen Schutz zu gewährleisten.
C) Privatsphäre ist das Recht, persönliche Angelegenheiten geheim zu halten. Datenschutz ist das Recht, personenbezogene Daten geheim zu halten.
D) Die Begriffe „Privatsphäre“ und „Datenschutz“ sind austauschbar. Hinsichtlich der Bedeutung gibt es keinen wirklichen Unterschied.

A) Falsch. Privatsphäre ist ein Recht, Datenschutz ist das Mittel, um dieses zu gewährleisten.
B) Richtig. Siehe: White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions.
C) Falsch. Privatsphäre ist ein Recht, Datenschutz ist das Mittel, um dieses zu gewährleisten.
D) Falsch. Privatsphäre ist ein Recht, Datenschutz ist das Mittel, um dieses zu gewährleisten.

36 / 40
Verordnung (EU) 2016/679, die als Datenschutz-Grundverordnung (DSGVO) bekannt ist, hebt eine frühere EU-Richtlinie auf.

Welche Richtlinie wird aufgehoben (ersetzt)?

A) Richtlinie 2002/58/EG vom 12. Juli 2002
B) Richtlinie 2006/24/EG vom 15. März 2006
C) Richtlinie 95/46/EG vom 24. Oktober 1995
D) Richtlinie 97/66/EG vom 15. Dezember 1997

A) Falsch. Richtlinie 2002/58/EG ergänzt einige Teile der Richtlinie 97/66/EG.
B) Falsch. Diese Richtlinie behandelt die Vorratsspeicherung von Daten, die beispielsweise von Internetanbietern erhoben werden.
C) Richtig. Diese Aufhebung ist im (Unter-)Titel der Verordnung angeführt. Quelle: DSGVO.
D) Falsch. Diese Richtlinie ergänzt Richtlinie 95/46/EG, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten in den Mitgliedstaaten zu gewährleisten.

37 / 40
Welches Recht von betroffenen Personen wird in der Datenschutz-Grundverordnung (DSGVO) ausdrücklich definiert?

A) Es muss eine Kopie der personenbezogenen Daten in dem von der betroffenen Person gewünschten Format bereitgestellt werden.
B) Kostenloser Zugriff der betroffenen Person auf personenbezogene Daten.
C) Personenbezogene Daten müssen auf Anfrage der betroffenen Person immer geändert werden.
D) Personenbezogene Daten müssen jederzeit gelöscht werden, wenn eine betroffene Person dies fordert.

A) Falsch. Sie müssen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, jedoch nicht notwendigerweise in einem von der betroffenen Person spezifizierten Format.
B) Richtig. Es muss allerdings nur die erste Kopie kostenlos zur Verfügung gestellt werden. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 3.
C) Falsch. Nur fehlerhafte Daten müssen berichtigt werden.
D) Falsch. Artikel 17 führt einige diesbezügliche Ausnahmen an, so z. B. wenn die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind.

38 / 40
Die Datenschutz-Grundverordnung (DSGVO) unterscheidet „sensible personenbezogene Daten“ als besondere Kategorie personenbezogener Daten.

Was ist ein Beispiel für solche Daten?

A) Ein Termin in einem Krankenhaus bei einem Facharzt
B) Eine internationale Bankkontonummer (IBAN)
C) Ein Abonnement einer politikwissenschaftlichen Zeitschrift
D) Die Mitgliedschaft in einem Branchenverband

A) Richtig. Termine bei einem Facharzt sind „personenbezogene Gesundheitsdaten“. Siehe: Art. 9.1 der DSGVO.
B) Falsch. IBAN-Nummern sind Daten, die sich eindeutig auf eine Person beziehen, d. h. personenbezogene Daten. Es sind jedoch keine sensiblen personenbezogenen Daten nach Art. 9 der DSGVO.
C) Falsch. Abonnements von politikwissenschaftlichen Zeitschriften sind keine „personenbezogenen Daten, aus denen politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen“ und somit keine sensiblen personenbezogenen Daten nach Art. 9 der DSGVO.
D) Falsch. Nur die Gewerkschaftszugehörigkeit und andere personenbezogene Daten, aus denen (...) politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, sind nach Art. 9 der DSGVO sensible personenbezogene Daten.

39 / 40
Welche Rolle im Datenschutz legt den Zweck und die Mittel der Verarbeitung personenbezogener Daten fest?

A) Verantwortlicher
B) Datenschutzbeauftragter
C) Auftragsverarbeiter

A) Richtig. Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Siehe: White Paper – Privacy, Personal Data and the GDPR - §1.4 Roles, responsibilities, stakeholders.
B) Falsch. Die DSGVO definiert den Datenschutzbeauftragten wie folgt: „Der Verantwortliche oder der Auftragsverarbeiter sollte bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden."
C) Falsch. Der Auftragsverarbeiter ist die Person oder Organisation, die personenbezogene Daten verarbeitet, aber nicht notwendigerweise die Person, die Zweck und Mittel festlegt.

40 / 40
Welche Informationen werden nach der Datenschutz-Grundverordnung (DSGVO) als personenbezogene Daten erachtet?

A) Informationen über eine Person, die die Privatsphäre dieser Person verletzen könnten, auch wenn sie falsch sind
B) Sämtliche Informationen hinsichtlich einer identifizierbaren natürlichen Person
C) Informationen hinsichtlich einer identifizierbaren natürlichen Person, die digitalisiert sind

A) Falsch. Sämtliche Aussagen über eine identifizierbare natürliche Person sind nach der DSGVO personenbezogene Daten.
B) Richtig. Siehe: EU-DSGVO, eine Kurzanleitung – Kapitel 2 und Art. 4(1) der DSGVO.
C) Falsch. Sämtliche Aussagen über eine identifizierbare natürliche Person sind nach der DSGVO personenbezogene Daten.

Beurteilung

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

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

Kontakt EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER