



Datenschutzbeauftragter

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

**Unlock the full bank of 562 questions
+ unlimited timed mock exams + mistake book**

Practice on the web: <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99 / week · \$6.99 / month · cancel anytime

What you unlock: all 562 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



Practice Questions

Try all 30 first, then check the answer key at the back.

Want the other 532+ questions & full timed mock exams? Unlock at
<https://certs.theorypractice.app/datenschutzbeauftragter>

1. Ist die Kommunikation zwischen Ihrem Browser und dem Zielsever verschlüsselt, ist es für Angreifer nahezu unmöglich die Verbindungsdaten mitzulesen.

- A. Richtig
- B. Falsch

2. Phishing-E-Mails mit manipulierten Links gibt es selten und die Zielseiten sind oft schlecht gemacht.

- A. Richtig
- B. Falsch

3. Beim Datenschutz geht es um ...

- A. den Schutz von Menschen.
- B. das Recht auf informationelle Selbstbestimmung,
- C. das Recht, selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen.
- D. die Erfüllung konkreter Unternehmensinteressen.

Study offline on the free app — search your exam on the App Store or Google Play

4. Was bedeutet „IT-Sicherheit“?

- A. IT-Sicherheit befasst sich mit dem Schutz von Daten, die in elektronischer Form gespeichert und verarbeitet werden.
- B. IT-Sicherheit ist ein Teilgebiet der Informationssicherheit.
- C. IT-Sicherheit befasst sich mit dem Schutz aller Assets vor Manipulationen, Verlust und unberechtigter Kenntnisnahme.
- D. IT-Sicherheit schützt persönliche Daten vor Verlust, Zerstörung oder Verfälschung.

5. Warum können Apps für die IT-Sicherheit gefährlich sein?

- A. Sie können unnötige Zugriffe und Berechtigungen auf das Smartphone haben.
- B. Sie können das Smartphone überlasten.
- C. Sie können mit ihren Funktionen überfordern.
- D. Sie können störende Werbung enthalten.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



6. Ein Passwort ist komplex, wenn es ...

- A. Groß- und Kleinschreibung enthält.
- B. Zahlen und Sonderzeichen enthält.
- C. über 12 Zeichen lang ist.
- D. über 8 Zeichen lang ist.

Want the other 532+ questions & full timed mock exams? Unlock at

<https://certs.theorypractice.app/datenschutzbeauftragter>

7. Welche Grundprinzipien müssen im Datenschutzrecht gemäß BDSG beachtet werden?

- A. Datenverarbeitungsverbot mit Erlaubnisvorbehalt
- B. Erforderlichkeitsprinzip
- C. Zweckbindung
- D. Direkterhebung

8. Über das Telefon verschaffen sich Angreifer zunächst oft ...

- A. Daten über die Unternehmensstruktur (Organigramm).
- B. über firmeninterne Termine.
- C. über Personen, mit denen er sich als Kollege oder Partner ausgeben kann.
- D. über Bezeichnungen, Nummern und Abkürzungen für Abteilungen oder Prozesse.

9. Welches Schadprogramm befiel mehrere Millionen Computer und verschlüsselte innerhalb von nur drei Tagen Daten auf mehr als 200.000 Windows-Rechnern in über 150 Ländern?

- A. WannaCry
- B. WannaSpy
- C. WannaPlay
- D. WannaScare

Study offline on the free app — search your exam on the App Store or Google Play

10. Eine Meldung ist laut Art. 33 DSGVO nicht erforderlich, wenn ein geringes Verletzungsrisiko der personenbezogenen Daten besteht.

- A. Richtig
- B. Falsch



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



11. Was stellt eine Verletzung der Rechte von betroffenen Personen dar?

- A. Die Weitergabe von Daten an Dritte ohne Rechtsgrundlage.
- B. Die Verarbeitung von personenbezogenen Daten mit Einwilligung.
- C. Die Verarbeitung von personenbezogenen Daten ohne Rechtsgrundlage.
- D. Nur ein Verlust von personenbezogenen Daten stellt eine Verletzung der Rechte dar.

12. Wie sind die Datenschutzbehörden in Deutschland organisiert?

- A. Der Bundesdatenschutzbeauftragte koordiniert die Arbeit der Landesbehörden.
- B. Jedes Bundesland hat mindestens eine Aufsichtsbehörde.
- C. Jede Landesbehörde darf frei entscheiden, wie Beschlüsse zu treffen sind.
- D. Jede der Datenschutz-Aufsichtsbehörden muss sich an das Kohärenzverfahren halten.

Want the other 532+ questions & full timed mock exams? Unlock at <https://certs.theorypractice.app/datenschutzbeauftragter>

13. Der Datenschutz soll jedem Unternehmen Schutz vor missbräuchlicher Datenverarbeitung und den Schutz der Privatsphäre garantieren.

- A. Richtig
- B. Falsch

14. Was müssen Verantwortliche und Auftragsverarbeiter zur Sicherheit der Verarbeitung berücksichtigen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

- A. Stand der Technik und Implementierungskosten
- B. Art, Umfang, Umstände der Verarbeitung personenbezogener Daten
- C. Zwecke der Verarbeitung personenbezogener Daten
- D. Eintrittswahrscheinlichkeit von Datenschutzvorfällen

15. Achten Sie darauf, dass Ihre Kollegen keine personenbezogenen Daten ohne Rücksprache mit Ihnen als DSB in Projekte oder an Datenverarbeiter außerhalb der EU senden!

- A. Richtig
- B. Falsch

Study offline on the free app — search your exam on the App Store or Google Play



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



16. Freiwilligkeit kann dann vorliegen, wenn ...

- A. für die beschäftigte Person ein rechtlicher Vorteil besteht.
- B. für die beschäftigte Person ein wirtschaftlicher Vorteil besteht.
- C. Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.
- D. für den Arbeitgeber ein wirtschaftlicher Vorteil besteht.

17. Welche Aufgaben besitzt ein Datenschutzbeauftragter?

- A. Er sollte Kenntnis über sämtliche Datenschutzregelungen und deren Auslegung durch aktuelle Gerichtsentscheidungen haben
- B. Kontrolle und Überwachung der Abläufe auf die Einhaltung der Datenschutzbestimmungen hin
- C. Schulungen der Mitarbeiter
- D. Kontrolle und Wahrung der Rechte Betroffener

18. Wie informieren Sie innerhalb Ihres Unternehmens am besten über Ihre Tätigkeit als Datenschutzbeauftragter sowie wichtige datenschutzrechtliche Themen?

- A. Ich rufe jeden Mitarbeiter einmal persönlich an, das genügt.
- B. Ich erstelle einen Aushang mit meinen Kontaktdaten für das schwarze Brett / Intranet.
- C. Ich erstelle einen kurzen Infobrief mit wichtigen datenschutzrechtlichen Neuigkeiten und Tipps.
- D. Ich schule die Mitarbeiter zu den Belangen des Datenschutzes.

Want the other 532+ questions & full timed mock exams? Unlock at
<https://certs.theorypractice.app/datenschutzbeauftragter>

19. Die Datenschutz-Folgeabschätzung (DSFA) ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht.

- A. Richtig
- B. Falsch

20. Welche dieser Daten gehören in die besondere Kategorie von personenbezogenen Daten?

- A. Religionszugehörigkeit
- B. E-Mailadresse
- C. Geburtsdatum
- D. Anschrift



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



21. Die Kundendaten eines Handelsunternehmens mit Niederlassung in Belgien werden vom Mutterkonzern in Japan gespeichert. Ist die DSGVO anwendbar?

- A. Ja, weil das Unternehmen eine Niederlassung in einem EU-Staat hat.
- B. Nein, weil die Daten in Japan gespeichert werden.
- C. Ja, weil die DSGVO europaweit gilt.
- D. Ja, weil es Ausnahmen für den Mutterkonzern gibt.

Study offline on the free app — search your exam on the App Store or Google Play

22. Mit welchem dieser Newsletter WordPress Plugin Anbieter ist ein AV bzw. ADV Vertrag erforderlich?

- A. MailChimp Plugin
- B. Email Subscribers & Newsletters Plugin
- C. Newsletter Plugin
- D. Email Subscribers

23. Wer gilt in einem Unternehmensbereich als sogenannte Dritte?

- A. Kunden
- B. Reinigungsdienst
- C. Kolleg/innen nicht involvierter Abteilungen
- D. Kolleg/innen der gleichen Abteilung

24. Menschliche Ursachen während der selbstständigen Arbeit sind:

- A. E-Mailsendungen an falsche Empfänger
- B. Unverschlossene Büros/nicht gesperrte PC-Bildschirme
- C. Wichtige Dokumente am falschen Drucker ausdrucken
- D. Elementare Gefahren wie Stromausfall, Brände und Überschwemmungen

Want the other 532+ questions & full timed mock exams? Unlock at

<https://certs.theorypractice.app/datenschutzbeauftragter>

25. Bei einem Datenschutzvorfall sind personenbezogene Daten betroffen und die Geschädigte ist demnach die natürliche Person.

- A. Richtig
- B. Falsch



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



26. Wie können Sie sich vor Sicherheitsvorfällen schützen?

- A. Benutzerkennungen nicht weitergeben und sichere Passwörter verwenden
- B. Lang unbesetzte Räume abschließen
- C. Arbeitsplatzrechner sperren durch „Windowstaste“ + „L“
- D. Auf dem richtigen Drucker drucken

27. Was müssen Sie beim Umgang mit öffentlichen und internen Dokumenten beachten?

- A. Intern klassifizierte Papierdokumente müssen regelmäßig aus Druckern und Faxgeräten entfernt werden.
- B. Interne Dokumente haben keinen Schutzbedarf.
- C. Öffentliche Dokumente haben einen normalen Schutzbedarf.
- D. Ich muss die Dokumente in einem Tresor aufbewahren.

Study offline on the free app — search your exam on the App Store or Google Play

28. Welche Hinweise müssen gemäß Art. 5 DSGVO für jede Verarbeitung beachtet werden?

- A. Verarbeitung nur mit Rechtsgrundlage!
- B. Verarbeitung nur nach zuvor definiertem Zweck!
- C. Daten müssen sachlich richtig und auf dem neuesten Stand sein!
- D. Daten müssen vor unbefugter Verarbeitung, Kenntnisaufnahme und Zerstörung geschützt werden!

29. Welche Anforderung beinhaltet das Arbeiten im Home-Office?

- A. Home-Office bedeutet zeitlich flexibles aber ortsgebundenes Arbeiten.
- B. Ihr dienstlicher Arbeitsbereich muss in Ihrem Privatbereich bereitgestellt und eingerichtet werden.
- C. Sie können im Home-Office Ihre Arbeit zeitlich flexibel erbringen.
- D. Es gelten die gleichen Anforderungen an die Informationssicherheit und den Datenschutz wie beim mobilen Arbeiten.

30. E-Mails sind – neben dem Telefon - das am wenigsten genutzte Kommunikationsmittel in Unternehmen.

- A. Richtig
- B. Falsch



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



Answer Key & Explanations

You just practised 30 of 562. Unlock every question + timed mocks at
<https://certs.theorypractice.app/datenschutzbeauftragter>

1. A — Richtig

****Diese Aussage ist richtig.**** Ist die Kommunikation zwischen Ihrem Browser und dem Zielsever verschlüsselt, ist es für Angreifer nahezu unmöglich die Verbindungsdaten mitzulesen. ****Weiterführende Informationen:**** Bei der SSL-Verschlüsselung wird der Datenverkehr auf der gesamten Strecke zwischen der Webseite und dem Browser des Nutzers verschlüsselt. Eine SSL-Verschlüsselung kann allerdings nur zur Anwendung kommen, wenn die betreffende Webseite diese Technik auch anbietet. Glücklicherweise gibt es kaum noch seriöse Webseiten ohne HTTPS.

2. A — Richtig

****Diese Aussage ist richtig.**** Phishing-E-Mails mit manipulierten Links gibt es ****häufig**** und die Zielseiten sind oft ****perfekt**** gemacht. ****Weiterführende Informationen:**** Grundsätzlich entscheiden Sie beim Browsen, welche Webseite Sie aufrufen wollen. Das klingt banal, beinhaltet aber eine wichtige Aussage – Seien Sie sich sicher, wo Sie sich befinden! Das größte Risiko ist nicht der Hacker, der Ihren Datenverkehr belauscht, sondern der Hacker der ihnen vormacht, dass Sie sich auf der Seite Ihrer Bank, der Bahn, der Seite des ÖVPN befinden – während Sie tatsächlich gerade auf einer täuschend ähnlichen Kopie Ihre Kontodaten eingeben. Lassen Sie sich nicht verleiten, auf Links in E-Mails oder Chatprogrammen einfach zu „klicken“. Sie wissen nicht, wohin Sie geschickt werden.

3. A — den Schutz von Menschen.

****Korrekte Antwort(en):**** * den Schutz von Menschen. * das Recht auf informationelle Selbstbestimmung, * das Recht, selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen. ****Weiterführende Informationen:**** Beim Datenschutz geht es um den Schutz von Menschen und deren Recht auf informationelle Selbstbestimmung, also dem Recht, selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen. Hier sind konkrete ****gesetzliche Vorgaben zwingend**** zu erfüllen, die sich im Wesentlichen aus der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) ergeben. Die DGSVO beschreibt das Ziel des Datenschutzes im Recht des Einzelnen auf Schutz seiner personenbezogenen Daten. Beim Datenschutz geht es nicht um den Schutz von allgemeinen Daten vor Schäden, sondern um den Schutz personenbezogener Daten vor Missbrauch („Datenschutz ist Personenschutz“). Der Schutz personenbezogener Daten stützt sich auf das Prinzip der informationellen Selbstbestimmung. Diese wurde im BVerfG-Urteil zur Volkszählung festgeschrieben. Geschützt werden muss dabei die Privatsphäre, d. h. Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben.

4. A — IT-Sicherheit befasst sich mit dem Schutz von Daten, die in elektronischer Form gespeichert und verarbeitet werden.

****Korrekte Antwort(en):**** * IT-Sicherheit befasst sich mit dem Schutz von Daten, die in elektronischer Form gespeichert und verarbeitet werden. * IT-Sicherheit ist ein Teilgebiet der Informationssicherheit. * IT-Sicherheit befasst sich mit dem Schutz aller Assets vor Manipulationen, Verlust und unberechtigter Kenntnisnahme. ****Weiterführende Informationen:**** IT-Sicherheit ist ein Teilgebiet der Informationssicherheit, die sich mit dem Schutz aller Daten und Informationen („Assets“) eines Unternehmens vor Manipulationen,



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



Verlust, unberechtigter Kenntnisnahme befasst. Der IT-Sicherheit kommt eine Schlüsselrolle für die Sicherheit von soziotechnischen Systemen zu. IT oder auch ITK-Systeme sind Teil der soziotechnischen Systeme. Zu den Aufgaben der IT-Sicherheit gehören der Schutz von ITK-Systeme von Organisationen gegen Bedrohungen. Damit soll unter anderem wirtschaftlicher Schaden verhindert werden. In Abgrenzung zu IT-Sicherheit umfasst Informationssicherheit neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

5. A — Sie können unnötige Zugriffe und Berechtigungen auf das Smartphone haben.

****Korrekte Antwort:**** * Sie können unnötige Zugriffe und Berechtigungen auf das Smartphone haben.

****Weiterführende Informationen:**** Die Telearbeit (auch Mobilarbeit oder mobile Arbeit) ist eine Arbeitsorganisation, bei der Arbeitnehmer ihre Arbeitsaufgaben ganz oder teilweise außerhalb der Geschäftsräume oder Betriebsstätten des Arbeitgebers überwiegend durch Telekommunikation ausüben.

6. A — Groß- und Kleinschreibung enthält.

****Korrekte Antwort(en):**** * Groß- und Kleinschreibung enthält. * Zahlen und Sonderzeichen enthält. * über 12 Zeichen lang ist. ****Weiterführende Informationen:**** Weniger als 12 Zeichen gelten aktuell als unsicher.

Sobald ein Passwort aufgeschrieben wird, ist es nicht mehr sicher und muss regelmäßig gewechselt werden. Es muss sich dabei signifikant vom vorherigen Passwort unterscheiden – mindestens 3 Zeichen müssen verändert werden. Wichtiger als der Wechsel ist aber die Passwortlänge und Komplexität. Passwörter

müssen immer sofort gewechselt werden, wenn der Verdacht besteht, dass die Sicherheit kompromittiert wurde, wie z. B. bei Verlust von mobilen Geräten.

7. A — Datenverarbeitungsverbot mit Erlaubnisvorbehalt

****Korrekte Antwort(en):**** * Datenverarbeitungsverbot mit Erlaubnisvorbehalt * Erforderlichkeitsprinzip * Zweckbindung * Direkterhebung ****Weiterführende Informationen:**** Das BDSG gilt für die Verarbeitung

personenbezogener Daten öffentlicher Stellen des Bundes und der Länder (soweit nicht landesrechtliche Regelungen greifen) sowie für nichtöffentliche Stellen. Es besteht aus vier Teilen: Gemeinsame Bestimmungen, Durchführungsbestimmungen zur DS-GVO, Datenschutzbestimmungen für Polizei- und Justizbehörden und Besondere Bestimmungen für Tätigkeiten außerhalb von DS-GVO und JI-Richtlinie.

****Quelle:**** IHK Weiterbildung - Geprüfte Fachwirte im Gesundheits- und Sozialwesen, Gestalten von Schnittstellen und Projekten (2016), Organisieren und Gestalten der Kommunikation zwischen den Berufsgruppen und von multiprofessioneller Teamarbeit, Seite 34

8. A — Daten über die Unternehmensstruktur (Organigramm).

****Korrekte Antwort(en):**** * Daten über die Unternehmensstruktur (Organigramm). * über firmeninterne

Termini. * über Personen, mit denen er sich als Kollege oder Partner ausgeben kann. * über Bezeichnungen, Nummern und Abkürzungen für Abteilungen oder Prozesse. ****Weiterführende Informationen:**** Angreifer

nutzen auch das Telefon als Mittel zum Angriff. Oft baut der Angreifer eine persönliche Beziehung zum Opfer auf, indem er mehrmals anruft, sich Schritt für Schritt ein Bild aufbaut und erst nach einiger Zeit nach

bestimmten Informationen fragt. In größeren Unternehmen sind solche Angriffe aussichtsreich, da sich der Angreifer leicht als Mitarbeiter einer anderen Abteilung oder aus einem anderen Standort ausgeben kann,

ohne dass der Angerufene sofort Verdacht schöpft. Aber selbst in kleineren Strukturen ist so etwas möglich, dort ist der Angreifer dann der vermeintliche externe Dienstleister oder Berater. Weil grundsätzlich jeder

getäuscht werden kann, ist es besonders wichtig, vorgeschriebene Wege und Prozeduren (etwa bei technischen Problemen oder der Informationsweitergabe) einzuhalten und misstrauisch zu bleiben.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start



9. A — WannaCry

****Korrekte Antwort:**** * WannaCry ****Weiterführende Informationen:**** ****WannaCry**** betraf weltweit mehrere hunderttausend Windows-Systeme. Eine der größten bislang beobachteten Ransomware-Wellen beherrschte im Mai 2017 die Schlagzeilen: Anders als die häufige Bezeichnung Erpressungstrojaner vermuten ließ, handelte es sich bei WannaCry allerdings um einen Wurm, der sich selbstständig ohne Zutun der Nutzer auf Windows-Rechnern verbreitete. Der Infektionsmechanismus von WannaCry nutzte eine Sicherheitslücke im Windows-Betriebssystem aus, für die Microsoft bereits acht Wochen vor dem Ausbruch der Epidemie ein Software-Patch bereitgestellt hatte. Ein zeitnahes Aufspielen dieses Sicherheitsupdates hätte in vielen Fällen die WannaCry-Infektion und alle dadurch ausgelösten Schäden verhindern können.

10. A — Richtig

****Diese Aussage ist richtig.**** Eine Meldung ist laut Art. 33 DSGVO nicht erforderlich, wenn ein geringes Verletzungsrisiko der personenbezogenen Daten besteht. ****Weiterführende Informationen:**** Dies ist dann der Fall wenn sicher verschlüsselte Datenträger verloren gegangen sind, auf denen sich entsprechende Daten befinden. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die DSGVO legt also sowohl fest, wer den Datenschutzverstoß melden, als auch innerhalb welcher Frist die Meldung vorgenommen werden muss. Wer Verantwortlicher im Sinne der DSGVO ist, wird im Art. 4 Nr. 7 definiert. Dementsprechend ist derjenige verantwortlich, der über die Zwecke und Mittel der Verarbeitung entscheidet.

11. A — Die Weitergabe von Daten an Dritte ohne Rechtsgrundlage.

****Korrekte Antwort(en):**** * Die Weitergabe von Daten an Dritte ohne Rechtsgrundlage. * Die Verarbeitung von personenbezogenen Daten ohne Rechtsgrundlage. * Die Vermarktung und der Vertrieb von personenbezogenen Daten ohne Rechtsgrundlage. ****Weiterführende Informationen:**** Betroffene Personen haben das Recht auf eine Information bei Datenschutzverletzung mit hohem Risiko → Art. 12-23 DSGVO. Da jede natürliche Person ein Recht auf informationelle Selbstbestimmung hat, liegen die Pflichten auf der Seite der Unternehmen, um dieses sicherzustellen. Alle betroffenen Personen haben ein Auskunftsrecht bezüglich Ihrer Daten (§§ 19 und 34 BDSG). Unternehmen und öffentliche Stellen haben daher gemäß Datenschutz die Pflicht, Betroffene in Bezug auf ihre Daten über Folgendes zu informieren: * Umfang der gespeicherten Daten * Herkunft der Daten * Zweck der Speicherung * Gegebenenfalls ob und an wen die Informationen übermittelt wurden Des Weiteren haben Betroffene ein Recht auf Berichtigung, Löschung oder Sperrung ihrer Daten (§§ 20 und 35 BDSG). Die Berichtigung muss dann vorgenommen werden, wenn die gespeicherten Informationen unrichtig sind. Eine Löschung oder Sperrung muss zum Beispiel dann erfolgen, wenn eine Speicherung nicht zulässig war.

12. B — Jedes Bundesland hat mindestens eine Aufsichtsbehörde.

****Korrekte Antwort(en):**** * Jedes Bundesland hat mindestens eine Aufsichtsbehörde. * Jede der Datenschutz-Aufsichtsbehörden muss sich an das Kohärenzverfahren halten. * Die Datenschutzaufsichtsbehörden sind für den öffentlichen und nicht-öffentlichen Bereich zuständig.

13. B — Falsch

****Diese Aussage ist falsch.** Die richtige Aussage lautet: ****Der Datenschutz soll jedem ****Bürger**** Schutz vor missbräuchlicher Datenverarbeitung und den Schutz der Privatsphäre garantieren. ****Weiterführende****



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



Informationen:** Aus diesem Grund ist die Verarbeitung oder das Verwenden von personenbezogenen Daten vor allem zum gewerblichen Zweck grundsätzlich verboten, es sei denn die Verarbeitung wird durch eine rechtliche Grundlage gestattet oder es liegt eine ausdrückliche, rechtsgültige Einwilligung des Betroffenen vor. Die Verarbeitung personenbezogener Daten ist nur bedingt zulässig. Des Weiteren sollen, im Sinne der Datenschutzgrundsätze, in jedem Fall so wenige Daten wie möglich und nur mit der Kenntnis des Betroffenen erhoben werden. Sie unterliegen einer Zweckbindung und sind zu löschen, sobald der Zweck der Erhebung nicht mehr besteht. Außerdem sind technische und organisatorische Maßnahmen zu treffen, die eine missbräuchliche Datenverarbeitung verhindern. Diese Grundsätze sollen den Datenschutz innerhalb Deutschlands gewährleisten.

14. A — Stand der Technik und Implementierungskosten

Korrekte Antwort(en): * Stand der Technik und Implementierungskosten * Art, Umfang, Umstände der Verarbeitung personenbezogener Daten * Zwecke der Verarbeitung personenbezogener Daten * Eintrittswahrscheinlichkeit von Datenschutzvorfällen * Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen **Weiterführende Informationen:** Der Verantwortliche sollte geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Maßnahmen auch wirksam sind. Zum Nachweis der Einhaltung der DSGVO sollte der Verantwortliche Maßnahmen ergreifen, die insbesondere: * den Grundsätzen des Datenschutzes durch Technik (data protection by design) genügen und * durch datenschutzfreundliche Voreinstellungen (data protection by default) dazu beitragen. Diese Maßnahmen können darin bestehen: * Minimierung der Verarbeitung personenbezogener Daten * Schnellstmögliche Pseudonymisierung personenbezogener Daten * Transparenz bezüglich der Funktionen und Verarbeitung * Überwachung der Verarbeitung * Schaffung und Verbesserung von Sicherheitsfunktionen Näher spezifiziert werden diese Punkte in → Art. 32 DSGVO - Sicherheit der Verarbeitung: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

15. A — Richtig

Diese Aussage ist richtig. Achten Sie darauf, dass Ihre Kollegen keine personenbezogenen Daten ohne Rücksprache mit Ihnen als DSB in Projekte oder an Datenverarbeiter außerhalb der EU senden!
Weiterführende Informationen: Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



16. A — für die beschäftigte Person ein rechtlicher Vorteil besteht.

****Korrekte Antwort(en):**** * für die beschäftigte Person ein rechtlicher Vorteil besteht. * für die beschäftigte Person ein wirtschaftlicher Vorteil besteht. * Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. ****Weiterführende Informationen:**** Im Beschäftigungskontext ist eine Einwilligung schriftlich oder elektronisch gemäß § 26 BDSG einzuholen. Im Allgemeinen bestimmt das BDSG, dass personenbezogene Daten nur dann erhoben, verarbeitet und genutzt werden dürfen, wenn der Betroffene diesem Vorgang zugestimmt oder aber eine eindeutige Rechtsvorschrift dies erlaubt bzw. anordnet. Bezogen auf die Mitarbeiterdaten ist Arbeitnehmerdatenschutz § 26 BDSG-neu von großer Bedeutung. Dieser gewährt die Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten durch den Arbeitgeber.

17. A — Er sollte Kenntnis über sämtliche Datenschutzregelungen und deren Auslegung durch aktuelle Gerichtsentscheidungen haben

Korrekte Antwort(en): * Er sollte Kenntnis über sämtliche Datenschutzregelungen und deren Auslegung durch aktuelle Gerichtsentscheidungen haben * Kontrolle und Überwachung der Abläufe auf die Einhaltung der Datenschutzbestimmungen hin * Schulungen der Mitarbeiter * Kontrolle und Wahrung der Rechte Betroffener (IHK Weiterbildung – Geprüfte Logistikmeister, Prozesssteuerung und –optimierung (2017), Informations- und Kommunikationssysteme, Seite 79, 80)

18. B — Ich erstelle einen Aushang mit meinen Kontaktdaten für das schwarze Brett / Intranet.

19. A — Richtig

****Diese Aussage ist richtig.**** Die Datenschutz-Folgeabschätzung (DSFA) ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht. ****Weiterführende Informationen:**** Datenschutz-Folgeabschätzung (DSFA) ist eine in bestimmten Fällen vorgeschriebene, strukturierte Risikoanalyse zur Vorabbewertung der möglichen Folgen von Datenverarbeitungsvorgängen, die der Verantwortliche im Sinne des Datenschutzrechts vorzunehmen hat. Die DSFA ist in ****Art. 35** der Datenschutz-Grundverordnung (DSGVO)****** geregelt. Sie ist demnach durchzuführen, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

20. A — Religionszugehörigkeit

****Korrekte Antwort:**** * Religionszugehörigkeit ****Weiterführende Informationen:**** In die besondere Kategorie von personenbezogenen Daten gehören: Daten zu Gesundheit, Religionsbekenntnis, Parteizugehörigkeit, Fingerabdruck, sexuelle Orientierung u. a.

21. A — Ja, weil das Unternehmen eine Niederlassung in einem EU-Staat hat.

****Korrekte Antwort:**** * Ja, weil das Unternehmen eine Niederlassung in einem EU-Staat hat.

****Weiterführende Informationen:**** Rund um die Verhandlungen der Datenschutz-Grundverordnung kritisierten EU-Abgeordnete massives Lobbying von Seiten der US-Regierung und von US-amerikanischen IT-Unternehmen. Technologie-Unternehmen aus den USA fürchten demnach den negativen Einfluss der Verordnung auf ihre Niederlassungen in Europa und übten entsprechenden Druck auf die Regierung von US-Präsident Obama aus. So forderte der amerikanische EU-Botschafter William E. Kennard in einer Rede in Brüssel am 4. Dezember 2012, dass die zentralen Forderungen der Verordnung gestrichen werden müssen: das Löschen sämtlicher Daten einer Person aus den Unternehmensdatenbanken auf Wunsch und die ausdrückliche Einverständniserklärung einer Person, bevor ihre Daten überhaupt gesammelt werden dürfen.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



22. A — MailChimp Plugin

****Korrekte Antwort:**** * MailChimp Plugin ****Weiterführende Informationen:**** MailChimp speichert und verarbeitet, im Gegensatz zu den beiden anderen Plugins, Abonnennten Daten auf MailChimp Servern. Die Websitebetreiber benötigen deshalb einen ADV Vertrag mit MailChimp.

23. A — Kunden

****Korrekte Antwort(en):**** * Kunden * Reinigungsdienst * Kolleg/innen nicht involvierter Bereiche ****Weiterführende Informationen:**** Die Unterlagen sind dementsprechend vor allen Kollegen aus nicht involvierten Abteilungen zu schützen. Kunden sind Dritte, sie sollten keinen Einblick in Unterlagen anderer Kunden und Konditionen nehmen können. Der Reinigungsdienst, der bei Ihrer Abwesenheit ihren Schreibtisch reinigt und den Müll entsorgt ist Dritter. Oft kommt der Reinigungsdienst vor Arbeitsbeginn oder nach Arbeitsende. Diese Personen sind oft unbeaufsichtigt in Ihrem Büro, hätten also genügend Zeit, sich in Ihren Unterlagen umzuschauen.

24. A — E-Mailsendungen an falsche Empfänger

****Korrekte Antwort(en):**** * E-Mailsendungen an falsche Empfänger * Unverschlossene Büros/nicht gesperrte PC-Bildschirme * Wichtige Dokumente am falschen Drucker ausdrucken ****Weiterführende Informationen:**** Es wird Ihnen vielleicht zunächst banal vorkommen, über E-Mailsendungen an falsche Empfänger zu sprechen, unverschlossene Büros, beziehungsweise nicht gesperrte PC-Bildschirme oder das Ausdrucken wichtiger Dokumente im falschen Drucker. Die Folgen können allerdings dramatisch sein und leider passieren solche Fehler im schnellen Tempo des Arbeitens häufiger, als man denkt.

25. A — Richtig

****Diese Aussage ist richtig.**** Bei einem Datenschutzvorfall sind personenbezogene Daten betroffen und die Geschädigte ist demnach die natürliche Person. ****Weiterführende Informationen:**** Formal wird zwischen Datenschutz- und Informationssicherheitsvorfällen unterschieden. Beide Arten sind Sicherheitsvorfälle und können sowohl interne als auch externe Ursachen haben. Bei einem Datenschutzvorfall sind personenbezogenen Daten betroffen. Also zum Beispiel Personal- oder Kundendaten. Der Geschädigte ist demnach die betroffene natürliche Person. Bei Informationssicherheitsvorfällen sind die betroffenen Daten Unternehmenswerte, also zum Beispiel IT-Systeme, IT-Anwendungen oder Daten und Dokumente. Geschädigte ist das Unternehmen. In einem Unternehmen können verschiedene Sicherheitsvorfälle auftreten, die Schäden für das Unternehmen aber auch für die Kunden und Partner bedeuten können.

26. A — Benutzerkennungen nicht weitergeben und sichere Passwörter verwenden

****Korrekte Antwort(en):**** * Benutzerkennungen nicht weitergeben und sichere Passwörter verwenden * Lang unbesetzte Räume abschließen * Arbeitsplatzrechner sperren durch „Windowstaste“ + „L“ * Auf dem richtigen Drucker drucken * Daten/Dokumente sicher aufbewahren und vor Dritten fernhalten ****Weiterführende Informationen:**** Egal ob es um den Schutz vor einem Informationssicherheits- oder Datenschutzvorfall geht. Es gibt Verhaltensweisen, die die Wahrscheinlichkeit des Eintretens eines Sicherheitsvorfalls reduzieren: * Geben Sie niemals Ihre Benutzerkennungen weiter! * Schließen Sie Räume ab, die länger unbesetzt sind! * Sperren Sie Ihren Arbeitsplatzrechner durch die Windowstaste und den Buchstaben „L“ * Verwenden Sie sichere Passwörter! * Drucken Sie auf dem richtigen Drucker! * Verwahren Sie Daten, Datenträger und Ausdrucke stets sicher! * Vernichten Sie nicht mehr benötigte Dokumente! * Verwehren Sie Unbefugten Einsicht in vertrauliche Unterlagen!

27. A — Intern klassifizierte Papierdokumente müssen regelmäßig aus Druckern und Faxgeräten entfernt werden.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



****Korrekte Antwort(en):**** * Intern klassifizierte Papierdokumente müssen regelmäßig aus Druckern und Faxgeräten entfernt werden. ****Weiterführende Informationen:**** Öffentliche Dokumente haben ****keinen Schutzbedarf.**** Interne Dokumente haben ****einen normalen Schutzbedarf****. Hier würde der unberechtigte Zugang zu den Informationen das Unternehmen oder die Organisation in keiner Weise beeinträchtigen, da die Informationen öffentlich verfügbar sind. Die Information ist demnach für eine größere Gruppe von Mitarbeitern und ausgesuchten Dritten ohne gesonderte Schutzmaßnahmen verfügbar. Intern klassifizierte Papierdokumente müssen regelmäßig aus Druckern und Faxgeräten entfernt werden und dürfen ungeschützt nur in Räumen, zu denen die Allgemeinheit keinen Zugang hat, aufbewahrt werden. Solche Dokumente können auch im Home-Office oder Mobile Office entsprechend der Richtlinien verarbeitet werden. Die Entsorgung kann durch jeden Mitarbeiter entsprechend der Richtlinie „Datenträgerentsorgung“ erfolgen.

28. A — Verarbeitung nur mit Rechtsgrundlage!

****Korrekte Antwort(en):**** * Verarbeitung nur mit Rechtsgrundlage! * Verarbeitung nur nach zuvor definiertem Zweck! * Daten müssen sachlich richtig und auf dem neuesten Stand sein! * Daten müssen vor unbefugter Verarbeitung, Kenntnisnahme und Zerstörung geschützt werden! ****Weiterführende Informationen:**** Die DSGVO legt Grundsätze fest, die für jede Verarbeitung beachtet werden müssen und eine Rechenschaft verlangen: * ****Rechtmäßigkeit, Treu und Glauben, Transparenz**** → Verarbeitung nur mit Rechtsgrundlage! * ****Zweckbindung**** → Verarbeitung nur nach zuvor definiertem Zweck! * ****Datenminimierung**** → "So viele Daten wie nötig, so wenige wie möglich!" * ****Richtigkeit**** → Daten müssen sachlich richtig und auf dem neuesten Stand sein! * ****Speicherbegrenzung**** → Wenn der Zweck der Verarbeitung erfüllt ist, müssen Daten gelöscht werden. * ****Integrität, Vertraulichkeit**** → Daten müssen vor unbefugter Verarbeitung, Kenntnisnahme und Zerstörung geschützt werden! Es handelt sich hier um ein Verbot mit Erlaubnisvorbehalt. Jeder Mensch soll grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können. Eine Datenerhebung ist somit zulässig, wenn sie durch die DSGVO selbst oder durch eine andere Rechtsvorschrift wie z.B. Steuer- und Abgabenrecht erlaubt wird.

29. A — Home-Office bedeutet zeitlich flexibles aber ortsgebundenes Arbeiten.

****Korrekte Antwort(en):**** * Home-Office bedeutet zeitlich flexibles aber ortsgebundenes Arbeiten. * Ihr dienstlicher Arbeitsbereich muss in Ihrem Privatbereich bereitgestellt und eingerichtet werden. * Sie können im Home-Office Ihre Arbeit zeitlich flexibel erbringen. ****Weiterführende Informationen:**** Sie können im Home-Office zwar Ihre Arbeit zeitlich flexibel erbringen, das bedeutet aber nicht, dass Sie automatisch auch von unterwegs, zum Beispiel von Ihrem Laptop aus, arbeiten dürfen. Denn dann bewegen Sie sich im Bereich des mobilen Arbeitens. Die Unterscheidung ist wichtig, weil im Home-Office und beim mobilen Arbeiten unterschiedliche Anforderungen an die Informationssicherheit und den Datenschutz gelten.

30. B — Falsch

****Diese Aussage ist falsch. Die richtige Aussage lautet:**** E-Mails sind – neben dem Telefon - das ****am meisten**** genutzte Kommunikationsmittel in Unternehmen. ****Weiterführende Informationen:**** Das bedeutet aber nicht, dass E-Mails an sich auch sicher sind. Im Grunde genommen ist eine E-Mail vergleichbar mit einer mit Bleistift beschriebenen Postkarte. Sie sind genauso einfach abzufangen, zu lesen oder zu verändern. Deshalb gibt es technische Schutzmaßnahmen und natürlich auch organisatorische Regelungen, die Ihnen beim sicheren Umgang mit E-Mails helfen können. Schließlich hat das Unternehmen großes Interesse daran, dass die Kommunikation per E-Mail reibungslos aber auch vertraulich vonstatten gehen kann.



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body



Ready to pass?

Unlock the full Datenschutzbeauftragter bank, every explanation, and unlimited timed mock exams.

Scan to start practising

<https://certs.theorypractice.app/datenschutzbeauftragter>

Also on iOS & Android — search your exam name on the App Store or Google Play



Unlock all 562 questions + timed mock exams

→ <https://certs.theorypractice.app/datenschutzbeauftragter>

\$2.99/week or \$6.99/month · cancel anytime · scan to start