Vorbereitungshandbuch

Ausgabe 201809

Inhalt

1. Überblick

EXIN Privacy & Data Protection Practitioner (PDPP.DE)

Anwendungsbereich

Die Zertifizierung EXIN Privacy & Data Protection (Privatsphäre und Datenschutz) Practitionerprüft, ob ein Experte die europäische Gesetzgebung zum Datenschutz (Wahrung der Privatsphäre) und deren internationale Relevanz kennt und versteht. Darüber hinaus bewertet sie, ob der Experte in der Lage ist, dieses Wissen in seinem Arbeitsalltag anzuwenden.

Zusammenfassung

Die Menge der im Internet verfügbaren Informationen wächst explosionsartig. Unternehmen mü ssen daher Maßnahmen ergreifen, die die Privatsphäre von Personen und deren Daten schützen. Nicht ohne Grund entstehen derzeit in der EU, aber auch in den USA und anderen Regionen der Welt, viele neue Gesetze, die genau diese Aspekte regulieren.
Vor kurzem endete die Übergangsfrist der EU-Datenschutz-Grundverordnung (DSGVO) der Europäischen Kommission. Damit sind die konkreten Vorgaben der Verordnung für alle Organisationen verbindlich. Die Zertifizierung PDPP baut auf den Themen auf, die in der Foundation-Zertifizierung abgedeckt wurden. Sie behandelt vor allem die Entwicklung und Umsetzung von Richtlinien und Verfahren zur Einhaltung bestehender und neuer Gesetze, zur Anwendung von Datenschutzleitlinien und Best Practices und zum Aufbau eines Datenschutzmanagementsystems.

Kontext

Die Zertifizierung EXIN Privacy & Data Protection Practitioner (PDPP) ist Teil des EXIN-Qualifikationsprogramms Privacy & Data Protection.

Zielgruppe

Die Zertifizierung der Stufe Practitioner richtet sich insbesondere an Beauftragte für Datenschutz und Privatsphäre, Justitiare und Compliancebeauftragte, Sicherheitsbeauftragte, Business Continuity Manager, Data Controller, Datenschutzauditoren (intern und extern) sowie Personalmanager.

Diese Zertifizierung ist eine Zertifizierung auf fortgeschrittenem Niveau. Wir empfehlen den Kandidaten daher dringend zuerst die Zertifizierung EXIN Privacy and Data Protection Foundation zu erwerben.

Zertifizierungsvoraussetzungen

- Teilnahme an einer akkreditierten Schulung zum Privacy and Data Protection Practitioner einschließlich erfolgreiche Durchführung der praktischen Aufgabenstellungen.
- Erfolgreicher Abschluss der Prüfung EXIN Privacy and Data Protection Practitioner.

Einzelheiten zur Prüfung

Prüfungsart:	Multiple-Choice-Fragen
Anzahl der Fragen:	40
Mindestpunktzahl:	65%
Einsicht in Dokumentation/Notizen während der Prüfung:	Nein, lediglich Literatur C wird als Anhang zum digitalen Examen bereitgestellt und darf bei Bedarf genutzt werden. Bringen Sie Ihre eigene Kopie mit, falls das Examen auf Papier gemacht wird.
Elektronische Geräte/Hilfsmittel erlaubt:	Nein
Prüfungsdauer:	120 Minuten

Es gelten die EXIN Examen-Regeln und -Vorschriften.

Taxonomiestufen nach Bloom

Die EXIN Privacy & Data Protection Practitioner Zertifizierung testet Kandidaten auf Bloom Level 2, 3 und Level 4 nach der überarbeiteten Taxonomie von Bloom:

- Bloom Level 2: Verstehen - ein Schritt über das Wissen hinaus. Verstehen zeigt, dass Kandidaten verstehen, was präsentiert wird und bewerten können, wie der Unterrichtsstoff in ihrem eigenen Umfeld angewendet werden kann. Diese Art von Fragen soll zeigen, dass der Kandidat in der Lage ist, die richtige Beschreibung von Fakten und Ideen zu organisieren, zu vergleichen, zu interpretieren und auszuwählen.
- Bloom Level 3: Anwenden – diese Stufe zeigt, dass der Teilnehmer Inhalte in einem anderen als dem gelernten Kontext anwenden kann. Die Fragen zu dieser Lernstufe sollen zeigen, dass der Teilnehmer Probleme in neuen Situationen lösen kann, indem er das erworbene Wissen bzw. die gelernten Tatsachen, Techniken und Regeln auf eine andere oder neue Art anwendet. Die Fragen beschreiben in der Regel ein kurzes Szenario.
- Bloom Level 4: Analysieren – diese Stufe zeigt, dass der Teilnehmer gelernte Inhalte zum besseren Verständnis in ihre Bestandteile gliedern kann. Diese Lernzielstufe nach Bloom wird in erster Linie mit Hilfe praktischer Aufgabenstellungen geprüft. Praktische Aufgabenstellungen sollen nachweisen, dass der Teilnehmer Informationen prüfen und in ihre Bestandteile zerlegen kann, indem er Motive oder Ursachen identifiziert, Schlussfolgerungen trifft und Belege für allgemein gültige Aussagen findet.

Schulung

Präsenzstunden

Für diesen Kurs empfehlen wir 21 Präsenzstunden. Darin enthalten sind Gruppenarbeiten, Prü fungsvorbereitung und kurze Pausen, nicht jedoch die für Hausaufgaben, praktische Aufgabenstellungen, die Prüfung und Mittagspausen benötigte Zeit. Wir empfehlen auf die praktische Aufgabenstellung nicht mehr als maximal 8 Stunden zu verwenden. Die praktischen Aufgabenstellungen können außerhalb der Schulung durchgeführt werden. Eine Durchführung im Rahmen der Schulung ist bei einer Verlängerung der Schulungsdauer ebenfalls möglich. Möchte der Schulungsanbieter ebenfalls Zeit für die nationale Gesetzgebung im Bereich Privatsphäre und Datenschutz aufwenden, so sind hierfür zusätzlich zu den 21 empfohlenen Präsenzstunden weitere Schulungsstunden erforderlich.

Regelstudiendauer

120 Stunden, je nach Vorwissen.

Schulungsanbieter

Eine Liste der akkreditierten Schulungsanbieter finden Sie auf der Webseite von EXIN www.exin.com.

2. Prüfungsanforderungen

Die Prüfungsanforderungen sind im Einzelnen in den Prüfungsspezifikationen erläutert. Die unten dargestellte Tabelle listet die Themen des Moduls (Prüfungsanforderungen) und die Unterthemen (Prüfungsspezifikationen).

Prüfungs-anforderung	Prüfungsspezifikationen	Gewicht-ung
1. Datenschutzrichtlinien		**10%**
	1.1 Zweck Datenschutzrichtlinien in einer Organisation	5%
	1.2 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	5%
2. Management und Organisation des Datenschutzes		**35%**
	2.1 Phasen des Datenschutzmanagementsystems (DPMS)	35%
	2.2 Maßnahmenplan für Datenschutzbewusstsein[1]	0%
3. Die Rolle des Verantwortlichen, des Auftragsverarbeiters und des Datenschutzbeauftragten		**15%**
	3.1 Rolle des Verantwortlichen und des Auftragsverarbeiters	7.5%
	3.2 Rolle des Datenschutzbeauftragten	7.5%
4. Datenschutzfolgeabschätzung (DPIA)		**30%**
	4.1 Kriterien für eine Datenschutzfolgeabschätzung (DPIA)	15%
	4.2 Schritte einer DPIA	15%
5. Verletzung des Schutzes personenbezogener Daten, Meldung und Notfallmaßnahmen		**10%**
	5.1 Anforderungen der DSGVO bei Verletzungen des Schutzes personenbezogener Daten	5%
	5.2 Anforderungen an eine Meldung	5%
	Total	100%

[1] Spezifikation 2.2 ist derzeit noch nicht Teil der Prüfung, da die Fachliteratur diesbezüglich derzeit noch zu wenig Informationen enthält. Sie wird in einer späteren Version ergänzt

Prüfungsspezifikationen

1 Datenschutzrichtlinien

1.1 Der Kandidat versteht, welchen Zweck Datenschutzrichtlinien in einer Organisation erfüllen.
Der Kandidat kann…

1.1.1 erklären, welche Richtlinien und Verfahren eine Organisation braucht, um die Datenschutzgesetze zu erfüllen.

1.1.2 den Inhalt der Richtlinien erklären.

1.2 Der Kandidat weiß, was man unter Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen versteht.
Der Kandidat kann…

1.2.1 das Konzept des Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen erläutern.

1.2.2 die sieben Prinzipien des Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen beschreiben.

1.2.3 zeigen, wie die Prinzipien des Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen umgesetzt werden können.

2 Management und Organisation des Datenschutz

2.1 Der Kandidat kann die Phasen des Datenschutzmanagementsystems (DSMS) anwenden.
Der Kandidat kann…

2.1.1 zeigen, wie man Phase 1 des Datenschutzmanagementsystems (DSMS) anwendet: Datenschutz und Privatsphäre: Vorbereitung

2.1.2 zeigen, wie man Phase 2 des Datenschutzmanagementsystems (DSMS) anwendet: Datenschutz und Privatsphäre: Organisation

2.1.3 zeigen, wie man Phase 3 des Datenschutzmanagementsystems (DSMS) anwendet: Datenschutz und Privatsphäre: Entwicklung und Umsetzung

2.1.4 zeigen, wie man Phase 4 des Datenschutzmanagementsystems (DSMS) anwendet: Datenschutz und Privatsphäre: Governance

2.1.5 zeigen, wie man Phase 5 des Datenschutzmanagementsystems (DSMS) anwendet: Datenschutz und Privatsphäre: Bewertung und Verbesserung

2.2 Der Kandidat kann die Theorie des Maßnahmenplans anwenden, um das Datenschutzbewusstsein zu stärken.[2]
Der Kandidat kann…

2.2.1 einen Maßnahmenplan erstellen, der das Datenschutzbewusstsein in einer bestimmten Situation stärkt.

3 Die Rolle des Verantwortlichen, des Auftragsverarbeiters und des Datenschutzbeauftragten

3.1 Roles of the Controller and Processor

Der Kandidat kann…

3.1.1 die Aufgaben des Verantwortlichen übernehmen.

3.1.2 die Aufgaben des Auftragsverarbeiters übernehmen.

3.1.3 erklären, in welchem Verhältnis der Verantwortliche und der Auftragsverarbeiter in einer bestimmten Situation stehen

[2] Spezifikation 2.2 ist derzeit noch nicht Teil der Prüfung, da die Fachliteratur diesbezüglich derzeit noch zu wenig Informationen enthält. Sie wird in einer späteren Version ergänzt.

3.2 Der Kandidat kann die Rolle und Aufgaben des Datenschutzbeauftragten übernehmen.
Der Kandidat kann…
3.2.1 erklären, wann laut der DSGVO ein Datenschutzbeauftragter Pflicht ist.
3.2.2 die Rolle des Datenschutzbeauftragten übernehmen.
3.2.3 erklären, welche Stellung der Datenschutzbeauftragte gegenüber der Aufsichtsbehörde einnimmt.

4 Datenschutzfolgeabschätzung (DPIA)

4.1 Der Kandidat kann die Kriterien für eine Datenschutzfolgeabschätzung (DPIA) anwenden.
Der Kandidat kann…
4.1.1 die Kriterien für die Durchführung einer Datenschutzfolgeabschätzung (DPIA) anwenden.
4.1.2 die Ziele und Ergebnisse einer Datenschutzfolgeabschätzung (DPIA) beschreiben.

4.2 Der Kandidat kann die Schritte einer Datenschutzfolgeabschätzung (DPIA) anwenden.
Der Kandidat kann…
4.2.1 die Schritte einer Datenschutzfolgeabschätzung (DPIA) beschreiben.
4.2.2 in einer bestimmten Situation eine Datenschutzfolgeabschätzung (DPIA) durchführen.

5 Verletzung des Schutzes personenbezogener Daten, Meldung und Notfallmaßnahmen

5.1 Der Kandidat kann die Anforderungen der DSGVO bei Verletzungen des Schutzes personenbezogener Daten anwenden.
Der Kandidat kann…
5.1.1 bewerten, ob eine Verletzung des Schutzes personenbezogener Daten entsprechend der DSGVO vorliegt.

5.2 Der Kandidat kann die Anforderungen an eine Meldung erfüllen.
Der Kandidat kann…
5.2.1 eine Verletzung des Schutzes personenbezogener Daten an die Überwachungsbehörde melden.
5.2.2 eine Verletzung des Schutzes personenbezogener Daten an die betroffene Person melden.
5.2.3 beschreiben, welche Elemente laut der DSGVO dokumentiert werden müssen.

3. Liste der Grundbegriffe

Dieses Glossar enthält Begriffe, mit denen die Teilnehmern vertraut sein sollten.

Bitte beachten Sie, dass die Kenntnis dieser Begriffe alleine nicht ausreicht. Die Teilnehmer müssen diese Begriffe auch verstehen und mit Beispielen belegen können.

Englisch	Deutsch
adequate	angemessen
appropriate technical and organizational measures	geeignete technische und organisatorische Maßnahmen
audit • initial data (protection) audit • internal and external data (protection) audit	Audit • Daten(schutz)voraudit • internes und externes Daten(schutz)audit
authenticity	Authentizität
availability	Verfügbarkeit
awareness	Bewusstsein
benchmark	Benchmark (Maßstab)
binding	verbindlich
binding corporate rules	verbindliche interne Datenschutzvorschriften
biometric data	biometrische Daten
Bring Your Own Device (BYOD)	Bring Your Own Device (BYOD)
certification	Zertifizierung
certification bodies	Zertifizierungsstellen
child's consent	Einwilligung des Kindes
cloud computing	Cloud Computing
codes of conduct	Verhaltenskodex
collection of personal data (verb.)	Erfassung personenbezogener Daten
commission reports	Berichte der Kommission
complaint	Beschwerde
compliance	Konformität (Compliance)
conditions for consent	Bedingungen für die Einwilligung
consent	Einwilligung
Consistency	Kohärenz
consistency mechanism	Kohärenzverfahren
constitution	Verfassung
contract	Vertrag
controller	Verantwortlicher
cross-border processing	grenzüberschreitende Verarbeitung
data accuracy	Datengenauigkeit
data breach	Verletzung des Schutzes personenbezogener Daten
data classification system	Datenklassifikationssystem
data concerning health	Gesundheitsdaten
data controller	Verantwortlicher
data lifecycle management (DLM)	Datenlebenszyklusmanagement
data mapping	Datenmapping

data portability	Datenübertragbarkeit
data protection	Datenschutz
(data privacy) breach response plan / data privacy incident response plan	Notfallplan für Verletzungen des Schutzes personenbezogener Daten/Notfall für Datenschutzvorfälle
data protection authority (DPA)	Aufsichtsbehörde[3]
data protection by default / privacy by default	datenschutzfreundliche Voreinstellungen / privatsphärenfreundliche Einstellungen
data protection by design / privacy by design	Datenschutz durch Technikgestaltung / Privatsphäre durch Technikggestaltung
data protection impact assessment (DPIA) / privacy impact assessment (PIA)	Datenschutzfolgeabschätzung (DPIA) / Folgenabschätzung für die Wahrung der Privatsphäre
Data Protection Management System (DPMS) / Data Protection and Privacy Management System (DPMS)	Datenschutzmanagementsystem/Managementsystem für Datenschutz und Wahrung der Privatsphäre
data protection officer (DPO) • designation • position • tasks	Datenschutzbeauftragter • Bestellung • Stellung • Aufgaben
data protection policy	Datenschutzrichtlinie
data protection program	Datenschutzprogramm
data protection provisions	Datenschutzbestimmungen
data subject	betroffene Person
data subject access (facilities)	Zugang der betroffenen Person (Einrichtungen)(
data transfer	Datenübertragung
declaration of consent	Einwilligungserklärung
delegated acts and implementing acts • committee procedure	Delegierte Rechtsakte und Durchführungsrechtsakte • Ausschussverfahren
documentation obligation	Dokumentationspflicht
derogation	abweichende Regelung
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	Durchsetzungsverfahren • Geldbußen • verwaltungsrechtliche Sanktionen • Strafen • abschreckende Sanktionen • wirksame Sanktionen • verhältnismäßige Sanktionen
enterprise	Unternehmen
European Economic Area (EEA)	Europäischer Wirtschaftsraum (EWR)
EU types of legal act • decision • directive • opinion • recommendation • regulation	Rechtsakte der Europäischen Union • Beschluss • Richtlinie • Stellungnahme • Empfehlung • Verordnung

[3] Vor Einführung der DSGVO waren die nationalen Behörden der EU-Mitgliedsstaaten als Datenschutzbehörden für die Umsetzung der Datenschutzverordnung verantwortlich. Die DSGVO verwendet nun den Begriff Aufsichtsbehörde

European Data Protection Board • chair • confidentiality • independence • procedure • reports • secretariat • tasks	Europäische Datenschutzausschuss • Vorsitz • Vertraulichkeit • Unabhängigkeit • Verfahren • Berichte • Sekretariat • Aufgaben
European Data Protection Supervisor (EDPS)	Europäischer Datenschutzbeauftragter
European Union legal acts on data protection	Rechtsakte der Europäischen Union zum Datenschutz
exchange of information	Informationsaustausch
exemption	Ausnahme, Freistellung
explicit consent	ausdrückliche Einwilligung
filing system	Dateisystem
General Data Protection Regulation (GDPR)	Datenschutz-Grundverordnung (DSGVO)
genetic data	genetische Daten
governing body	leitende Stelle
group of undertakings	Unternehmensgruppe
incident response	Notfallmanagement, Reaktion auf Vorfälle
independent supervisory authorities • activity reports • competence • establishment • powers • tasks	unabhängige Aufsichtsbehörden • Tätigkeitsberichte • Kompetenz • Geltendmachung • Befugnisse • Aufgaben
Information Security Management System (ISMS)	Informationssicherheitsmanagementsystem (ISMS)
information society service	Dienst der Informationsgesellschaft
international organization	internationale Organisation
Internet of Things (IOT)	Internet der Dinge (Industrie 4.0)
joint controllers	gemeinsam Verantwortliche
judicial remedy	gerichtlicher Rechtsbehelf
lawfulness of processing	Rechtmäßigkeit der Verarbeitung
legal basis	Rechtsgrundlage
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)	berechtigter Grund (17/1c, 18/1d, 21/1) und zulässige Rechtsgrundlage (DSGVO 40)
legitimate interest	berechtigtes Interesse
liability	Haftung
main establishment	Hauptniederlassung
material scope	sachlicher Anwendungsbereich
measures based on DPIA results	Maßnahmen infolge der Datenschutzfolgeabschätzung (DPIA)
National Identification Number	nationale Kennziffer
non-repudiation	Nichtabstreitbarkeit
notification obligation	Meldepflicht
opinion of the board	Stellungnahme des Ausschusses
personal data	personenbezogene Daten

personal data breach	Verletzung des Schutzes personenbezogener Daten
personal data relating to criminal convictions and offences	personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten
principles relating to processing of personal data (Lit. C GDPR, Article 5) • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	Grundsätze für die Verarbeitung personenbezogener Daten • Rechenschaftspflicht • Richtigkeit, Korrektheit • Vertraulichkeit • Datenminimierung • Verarbeitung nach Treu und Glauben (Fairness) • Integrität • Rechtmäßigkeit • Zweckbindung • Speicherbegrenzung • Transparenz
policy	Politik
policy rule(s)	Regeln der Politik
prior consultation	vorherige Konsultation
privacy	Privatsphäre
privacy analysis	Datenschutzanalyse
privacy officer/chief privacy officer	Datenschutzbeauftragter/Konzerndatenschutzbeauftragter
processing	Verarbeitung
processing (of personal data)	Verarbeitung (personenbezogener Daten)
processing agreement	Vertrag zur Datenverabeitung
processing situations • data protection rules of churches and religious associations • employment • for archiving purposes in the public interest • for scientific or historical research purposes • for statistical purposes • freedom of expression and information • National Identification Number • obligations of secrecy • public access to official documents	Verarbeitungssituationen • Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften • Beschäftigung • für im öffentlichen Interesse liegende Archivzwecke • für wissenschaftliche oder historische Forschungszwecke • für statistische Zwecke • freie Meinungsäußerung und Information • nationale Kennziffer • Geheimhaltungspflichten • Zugang der Öffentlichkeit zu amtlichen Dokumenten
processing which does not require identification	Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist
processor	Auftragsverarbeiter
profiling	Profiling
proportionality, the principle of	Verhältnismäßigkeit, das Prinzip der
pseudonymization	Pseudonymisierung
quality cycle	Qualitätszyklus
recipient	Empfänger
relevant and reasoned objection	maßgeblicher und begründeter Einspruch

repealed	außer Kraft gesetzt
representative	Vertreter
restriction of processing	Einschränkung der Verarbeitung
retention period	Aufbewahrungsfrist
right to compensation	Recht auf Schadenersatz
rights of the data subject • automated individual decision-making • data portability • information and access • modalities • notification obligation • rectification and erasure • restriction of processing • restrictions • 'right to be forgotten' • right to objection • transparency	Rechte der betroffenen Person • automatisierte Entscheidungsfindung im Einzelfall • Datenübertragbarkeit • Informationspflicht und Recht auf Auskunft • Modalitäten • Mitteilungspflicht • Berichtigung und Löschung • Einschränkung der Verarbeitung • Einschränkungen • Recht auf Vergessenwerden • Widerspruchsrecht • Transparenz
risk management	Risikomanagement
rules of procedure	Geschäftsordnung
security breach (security incident)	Sicherheitsverstoß (Sicherheitsvorfall)
security of personal data	Sicherheit personenbezogener Daten
security of processing	Sicherheit der Verarbeitung
sensitive data	sensible Daten
service provider	Service Provider
seven principles for privacy by design (Lit. A Chapter 5, paragraph Privacy by design and by default)	Die sieben Prinzipien des Datenschutz durch Technikgestaltung ((Lit. A Kapitel 5, Absatz Privacy by design and by default)
Social, Mobile, Analytics, Cloud, Things (SMACT)	SMACT-Technologien (Social, Mobile, Analytics, Cloud, Internet of Things)
special categories of personal data • biometric data • data concerning health • genetic data • political opinions • racial or ethnic origin • religious or philosophical beliefs • sex life or sexual orientation • trade union membership	besondere Arten personenbezogener Daten • biometrische Daten • Gesundheitsdaten • genetische Daten • politische Einstellung • Rasse oder ethnische Herkunft • Religion oder Weltanschauung • Sexualleben oder sexuelle Orientierung • Gewerkschaftszugehörigkeit
subsidiarity, the principle of	Subsidiarität, Prinzip der
supervisory authority	Aufsichtsbehörde
supervisory authority concerned	betroffene Aufsichtsbehörde
suspension of proceedings	Aussetzung des Verfahrens
territorial scope	Räumlicher Anwendungsbereich
third party	Dritter
threat	Bedrohung

transfer of personal data to third countries and to international organizations • adequacy decision • appropriate safeguards • binding corporate rules • derogations • disclosures • international protection of personal data	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen • Angemessenheitsbeschluss • geeignete Sicherheitsvorkehrungen • verbindliche interne Datenschutzvorschriften • abweichende Regelung • Offenlegung • internationaler Schutz personenbezogener Daten
unified communications and collaboration (UCC)	Unified Communications and Collaboration (UCC)
vulnerability	Schwachstelle/Sicherheitslücke

4. Literatur

Fachliteratur zur Prüfung

Das für die Prüfung benötigte Wissen wird durch folgende Literatur abgedeckt.

A. IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide
IT Governance Publishing, Cambridgeshire (2016)
ISBN 978-1-84928-8354 (paperback)
ISBN 978-1-84928-8378 (e-book)

B. Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. 1
bookboon.com 1st edition (2016)
ISBN 978-87-403-1540-0

C. European Commission
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016, available at http://eur-lex.europa.eu
PDF:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
HTML:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

D. Article 29 Data Protection Working Party
Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01, 5 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (Deutsche Version unter 'Available language versions')

E. Article 29 Data Protection Working Party
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248, 4 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (Deutsche Version unter 'Available language versions')

Anmerkung

Die Prüfungsanforderungen basieren auf der Fachliteratur zur Prüfung. Die unter Punkt C angegebene DSGVO gilt nicht als primäre Fachliteratur zur Prüfung, da die sonstige Fachliteratur bereits genügend Informationen über die DSGVO bietet. Die Kandidaten sollten jedoch in dem Maße mit der DSGVO vertraut sein, in dem die weitere Fachliteratur zur Prüfung auf die DSGVO verweist. Die unter Punkt C angegebene Fachliteratur wird als Anhang zur Prüfung bereitgestellt und darf bei Bedarf konsultiert werden.

Weiterführende Literatur

F. Example of Privacy by Design Framework
https://www.privacycompany.eu/files/DPbD_Framework.pdf

Anmerkung

Die weiterführenden Literaturempfehlungen dienen lediglich zu Referenzzwecken und der weiteren Vertiefung des Wissens.

Literaturverzeichnis

Prüfungs-anforderung	Prüfungsspezifikation	Literatur
1. Datenschutzrichtlinien		
	1.1 Zweck Datenschutzrichtlinien in einer Organisation	A: Kap. 16, Abschnitt Using policies to demonstrate compliance
	1.2 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	A: Kap. 5, Abschnitt Privacy by design and by default
2. Management und Organisation des Datenschutzes		
	2.1 Phasen des Datenschutzmanagementsystems (DPMS)	A: Kap. 12, Abschnitt Records of processing A: Kap. 14, Einleitung + Abschnitt Notification B: Kap. 2, Abschnitt 2 DP&P System Phases
	2.2 Maßnahmenplan für Datenschutzbewusstsein	*Noch keine Literatur vorhanden*
3. Die Rolle des Verantwortlichen, des Auftragsverarbeiters und des Datenschutzbeauftragten		
	3.1 Rolle des Verantwortlichen und des Auftragsverarbeiters	A: Kap. 12
	3.2 Rolle des Datenschutzbeauftragten	A: Kap. 2 B: Kap. 2, Abschnitt 2 Phase 4 D: Kap. 2, Abschnitt 1 Mandatory designation D: Kap. 4 Tasks of the DPO D: Kap. 5, Abschnitt 1 Which organizations must appoint a DPO?
4. Datenschutzfolgeabschätzung (DPIA)		
	4.1 Kriterien für eine Datenschutzfolgeabschätzung (DPIA)	A: Kap. 5, Einleitung, Abschnitt Privacy Impact Assessments und Abschnitt When to conduct a DPIA A: Kap. 6, Abschnitt DPIA's as part of risk management A: Kap. 8, Abschnitt Objectives and outcomes E: Kap. 3 DPIA: the Regulation explained

	4.2 Schritte einer DPIA	A: Kap. 5, Abschnitt Privacy Impact Assessments A: Kap. 7 A: Kap. 8, Abschnitt Five key stages in a DPIA und Abschnitt Consultation E: Kap. 3 DPIA: the Regulation explained
5. Verletzung des Schutzes personenbezogener Daten, Meldung und Notfallmaßnahmen		
	5.1 Anforderungen der DSGVO bei Verletzungen des Schutzes personenbezogener Daten	A: Kap. 3, Abschnitt Personal data breaches, Anatomy of a data breach, Sites of attack A: Kap. 14, Abschnitt Notification, Abschnitt Events vs incidents, Abschnitt Types of incidents
	5.2 Anforderungen an eine Meldung	A: Kap. 14, Abschnitt Notification, Abschnitt Key roles in incident management, Abschnitt Respond und Abschnitt Follow up

Anmerkung

Literatur C, auf die DSGVO wird nicht im Einzelnen verwiesen.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER