EXIN Privacy & Data Protection

PRACTITIONER

Certified by EXIN

Preparation guide

Editie 201809

Inhoud

1. Overzicht

EXIN Privacy & Data Protection Practitioner (PDPP.NL)

Scope

EXIN Privacy & Data Protection Practitioner is een certificering die het kennisniveau van een professional, over het inzicht in de Europese privacy- (gegevensbeschermings-)wetgeving en de internationale relevantie hiervan bevestigt. Ook bevestigt de certificering het vermogen van de professional om deze kennis en inzicht in de dagelijkse beroepspraktijk toe te passen.

Samenvatting

Met de steeds toenemende explosie van informatie die het internet overspoelt, moet elk bedrijf het beheren en beschermen van de privacy van personen en hun gegevens organiseren. Er worden niet voor niets veel nieuwe wetten - zowel in de VS als in de EU en in veel andere regio's - gemaakt om beide te reguleren.
De Algemene Verordening Gegevensbescherming (AVG), die is gepubliceerd door de Europese Commissie en het Europees Parlement en toepasselijk recht is geworden in de EU, verplicht alle organisaties zich te houden aan strikte en gedetailleerde regels voor de bescherming van persoonsgegevens.
De EXIN Privacy & Data Protection Practioner certificering bouwt voort op de onderwerpen van het Foundation examen. Het richt zich op de ontwikkeling en implementatie van beleid en procedures om aan bestaande en nieuwe wetgeving te voldoen, op de toepassing van privacy- en gegevensbeschermingsrichtlijnen en best practices en op het opzetten van een managementsysteem voor privacy- en gegevensbescherming.

Context

De certificering EXIN Privacy and Data Protection Practitioner (PDPP) is onderdeel van het EXIN certificeringsprogramma EXIN Privacy and Data Protection.

Doelgroep

Deze certificering op Practitioner niveau is met name nuttig voor functionarissen voor gegevensbescherming (FG's), privacy officers, juridisch medewerkers en compliance officers, beveiligers, business continuity managers, verwerkingsverantwoordelijken, auditors voor gegevensbescherming (intern en extern), privacy analist en HR managers.
Aangezien dit een certificering op gevorderd niveau is, wordt sterk aanbevolen om basiskennis op te doen door het examen EXIN Privacy and Data Protection Foundation te behalen.

Certificeringseisen

- Geaccrediteerde Privacy & Data Protection Practitioner training, inclusief afronding van de praktijkopdrachten.
- Met goed gevolg afleggen van het examen EXIN Privacy & Data Protection Practitioner.

Examendetails

Examenvorm:	Multiple-choicevragen
Aantal vragen:	40
Cesuur:	65%
Open boek/notities:	Nee, met uitzondering van literatuur C. Literatuur C mag worden geraadpleegd tijdens het examen. Het wordt als appendix aangeboden bij digitale examens. Breng s.v.p. uw eigen exemplaar mee als het examen op papier wordt afgenomen.
Elektronische hulpmiddelen toegestaan:	Nee
Examenduur:	120 minuten

Op dit examen is het Reglement voor de examens van EXIN van toepassing.

Bloom level

De certificering EXIN Privacy & Data Protection Practitioner toetst kandidaten op Bloom Levels 2, 3 en 4 volgens Bloom's Revised Taxonomy:

- Bloom Level 2: Begrijpen – een stap hoger dan onthouden. Op dit niveau begrijpen kandidaten de aangeboden materialen en kunnen ze aangeven hoe ze deze in hun eigen omgeving kunnen toepassen. Met dit type vragen wordt bepaald of de kandidaat in staat is om feiten en ideeën te ordenen, te vergelijken, te interpreteren en correct te beschrijven.
- Bloom Level 3: Toepassen – laat zien dat kandidaten in staat zijn om informatie in een andere context te gebruiken dan die waarin deze is geleerd. Dit type vragen onderzoekt of de kandidaat in staat is problemen in nieuwe situaties op te lossen door verworven kennis, feiten, technieken en regels op een andere of nieuwe manier toe te passen. Deze vragen bevatten meestal een korte voorbeeldsituatie.
- Bloom Level 4: Analyseren – laat zien dat kandidaten in staat zijn geleerde informatie in stukjes op te breken om hem te begrijpen. Dit Bloom Level wordt voornamelijk getoetst middels de praktijkopdrachten. De praktijkopdrachten zijn bedoeld om te toetsen of de kandidaat kan onderzoeken en informatie in delen kan opbreken door redenen of oorzaken te herkennen, conclusies te trekken en bewijs te vinden voor generalisaties.

Training

Contacturen

Het aangeraden aantal contacturen tijdens de training is 21. Dit omvat praktijkopdrachten, voorbereiding op het examen en korte pauzes. Dit aantal uren is exclusief lunchpauzes, huiswerk en het examen.
De aanbevolen uren voor de praktijkopdrachten is maximaal 8. De praktijkopdrachten kunnen buiten de training gemaakt worden. Ze kunnen ook tijdens de training gedaan worden, als de duur van de training wordt verlengd.
Als de training provider tijd wil wijden aan nationale privacy en data protection wetgeving, zal dit extra trainingsuren vereisen bovenop de aanbevolen 21 uur.

Indicatie studielast

120 uur, afhankelijk van bestaande kennis.

Trainingsorganisatie

Een lijst van geaccrediteerde trainingsorganisaties kunt u vinden op de website van EXIN www.exin.com.

2. Exameneisen

De exameneisen staan vermeld in de examenspecificaties. De volgende tabel bevat de onderwerpen van de module (exameneisen) en de subonderwerpen (examenspecificaties).

Exameneis	Examenspecificatie	Gewicht
1. Gegevensbeschermingsbeleid		**10%**
	1.1 doel van het gegevensbeschermings-/privacybeleid binnen een organisatie	5%
	1.2 gegevensbescherming door ontwerp en door standaardinstellingen	5%
2. Gegevensbescherming beheren en organiseren		**35%**
	2.1 fases van het managementsysteem voor gegevensbescherming (DPMS)	35%
	2.2 actieplan voor bewustzijnsvorming over gegevensbescherming	0%
3. Rollen van de verwerkingsverantwoordelijke, verwerker en functionaris voor gegevensbescherming (FG)		**15%**
	3.1 rollen van de verwerkingsverantwoordelijke en verwerker	7.5%
	3.2 rol en verantwoordelijkheden van een FG[1]	7.5%
4. Gegevensbeschermingeffectenbeoordeling (DPIA)		**30%**
	4.1 criteria for a DPIA	15%
	4.2 stappen van een DPIA	15%
5. Inbreuken in verband met persoonsgegevens, melding van en reactie op inbreuken in verband met persoonsgegevens		**10%**
	5.1 vereisten van de AVG over inbreuken in verband met persoonsgegevens	5%
	5.2 vereisten voor melding	5%
	Totaal	100%

[1] Examenspecificatie 2.2 is niet opgenomen in het examen, omdat er op dit moment nog geen geschikt referentiemateriaal (literatuur) beschikbaar is. Examenvragen over dit onderwerp zullen in een latere versie worden opgenomen.

Examenspecificaties

1 Gegevensbeschermingsbeleid

1.1 Het doel van het gegevensbeschermings-/privacybeleid binnen een organisatie

De kandidaat kan…

1.1.1 uit te leggen welk beleid en procedures binnen een organisatie nodig zijn om aan de wetgeving inzake gegevensbescherming te voldoen.

1.1.2 de inhoud van het beleid uit te leggen.

1.2 Gegevensbescherming door ontwerp en door standaardinstellingen

De kandidaat kan…

1.2.1 uit te leggen wat het concept gegevensbescherming door ontwerp en door standaardinstellingen inhoudt.

1.2.2 de zeven principes voor gegevensbescherming door ontwerp en door standaardinstellingen te beschrijven.

1.2.3 te laten zien hoe principes voor gegevensbescherming door ontwerp en door standaardinstellingen kunnen worden geïmplementeerd.

2 Gegevensbescherming beheren en organiseren

2.1 Fasen van het managementsysteem voor gegevensbescherming (DPMS)

De kandidaat kan…

2.1.1 te laten zien hoe fase 1 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Voorbereiding.

2.1.2 te laten zien hoe fase 2 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Organisatie.

2.1.3 te laten zien hoe fase 3 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Ontwikkeling en implementatie.

2.1.4 te laten zien hoe fase 4 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Governance.

2.1.5 laten zien hoe fase 5 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Evaluatie en verbetering.

2.2 Een actieplan voor bewustzijnsvorming over gegevensbescherming[2]

De kandidaat kan…

2.2.1 een actieplan samen te stellen voor bewustzijnsvorming over gegevensbescherming in een specifieke situatie.

3 Rollen van de verwerkingsverantwoordelijke, verwerker en functionaris voor gegevensbescherming (FG)

3.1 Rollen van de verwerkingsverantwoordelijke en verwerker

De kandidaat kan…

3.1.1 de verantwoordelijkheden van de verwerkingsverantwoordelijke na te leven.

3.1.2 de verantwoordelijkheden van de verwerker na te leven.

3.1.3 de relatie tussen de verwerkingsverantwoordelijke en de verwerker uit te leggen voor een specifieke situatie.

[2] Examenspecificatie 2.2 is niet opgenomen in het examen, omdat er op dit moment nog geen geschikt referentiemateriaal (literatuur) beschikbaar is. Examenvragen over dit onderwerp zullen in een latere versie worden opgenomen.

3.2 De rol en verantwoordelijkheden van een FG

De kandidaat kan…

- 3.2.1 uit te leggen wanneer de AVG een FG verplicht stelt.
- 3.2.2 de rol van de FG na te leven.
- 3.2.3 de positie van de FG ten opzichte van de toezichthoudende autoriteit uit te leggen.

4 Gegevensbeschermingseffectbeoordeling (DPIA)

4.1 Criteria voor een DPIA

De kandidaat kan…

- 4.1.1 de criteria voor het uitvoeren van een DPIA toe te passen.
- 4.1.2 de doelen en uitkomsten van een DPIA te beschrijven.

4.2 De stappen van een DPIA

De kandidaat kan…

- 4.2.1 de stappen van een DPIA te beschrijven.
- 4.2.2 een DPIA uit te voeren in een specifieke situatie.

5 Inbreuken in verband met persoonsgegevens, melding van en reactie op inbreuken in verband met persoonsgegevens

5.1 Vereisten van de AVG over inbreuken in verband met persoonsgegevens

De kandidaat kan…

- 5.1.1 te beoordelen of volgens de criteria van de AVG een inbreuk in verband met persoonsgegevens heeft plaatsgevonden.

5.2 Vereisten voor melding

De kandidaat kan…

- 5.2.1 een inbreuk in verband met persoonsgegevens bij de toezichthoudende autoriteit te melden.
- 5.2.2 de betrokkenen op de hoogte te brengen van de inbreuk in verband met persoonsgegevens.
- 5.2.3 te beschrijven uit welke onderdelen de documentatieverplichting van de AVG bestaat.

3. Begrippenlijst

Dit hoofdstuk bevat de begrippen en afkortingen die kandidaten moeten kennen.

Let op! Uitsluitend kennis van deze termen is niet voldoende voorbereiding voor het examen; de kandidaten moeten de begrippen begrijpen en in staat zijn om voorbeelden te geven.

English	**Nederlands**
adequate	toereikend
appropriate technical and organizational measures	passende technische en organisatorische maatregelen
audit • initial data (protection) audit • internal and external data (protection) audit	audit • initiële audit van de gegevens(bescherming) • interne en externe audit van de gegevens(bescherming)
authenticity	authenticiteit
availability	beschikbaarheid
awareness	bewustzijn, besef
benchmark	benchmark (vergelijken / vergelijking met een standaard)
binding	bindend
binding corporate rules	bindende bedrijfsvoorschriften
biometric data	biometrische gegevens
Bring Your Own Device (BYOD)	Bring Your Own Device (BYOD ofwel breng je eigen apparaat mee)
certification	certificering
certification bodies	certificeringsorganen
child's consent	toestemming van kinderen
cloud computing	cloud computing
codes of conduct	gedragscodes
collection of personal data (verb.)	verzamelen van persoonsgegevens
commission reports	commissieverslagen
complaint	klacht
compliance	voldoen (aan)
conditions for consent	voorwaarden voor toestemming
consent	toestemming
consistency	coherentie
consistency mechanism	coherentiemechanisme
constitution	grondwet
contract	overeenkomst
controller	verwerkingsverantwoordelijke
cross-border processing	grensoverschrijdende verwerking
data accuracy	nauwkeurigheid van de gegevens
data breach	inbreuk in verband met persoonsgegevens
data classification system	systeem voor gegevensclassificatie
data concerning health	gegevens over gezondheid

data controller	verwerkingsverantwoordelijke
data lifecycle management (DLM)	data lifecycle management (DLM ofwel management van de levenscyclus van gegevens)
data mapping	koppelen van gegevens
data portability	gegevensoverdraagbaarheid
data protection	gegevensbescherming
(data privacy) breach response plan / data privacy incident response plan	reactieplan inbreuk persoonsgegevens (datalek) / reactieplan privacy-inbreuk
data protection authority (DPA)	toezichthoudende autoriteit (Nederland: ‘Autoriteit Persoonsgegevens’ - AP); (België: ‘Gegevensbeschermingsautoriteit’)
data protection by default / privacy by default	gegevensbescherming door standaardinstellingen / privacy door standaardinstellingen
data protection by design / privacy by design	gegevensbescherming door ontwerp / privacy door ontwerp
data protection impact assessment (DPIA) / privacy impact assessment (PIA)	gegevensbeschermingseffectbeoordeling (DPIA) / privacyeffectbeoordeling (PIA)
Data Protection Management System (DPMS) / Data Protection and Privacy Management System (DPMS)	Managementsysteem voor gegevensbescherming (DPMS) / Managementsysteem voor privacy- en gegevensbescherming (DPMS)
data protection officer (DPO) • designation • position • tasks	functionaris voor gegevensbescherming (FG) • aanwijzing • positie • taken
data protection policy	gegevensbeschermingsbeleid
data protection program	gegevensbeschermingsprogramma
data protection provisions	gegevensbeschermingsbepalingen
data subject	betrokkene
data subject access (facilities)	toegang(sfaciliteiten) voor de betrokkene
data transfer	doorgeven van persoonsgegevens
declaration of consent	toestemmingsverklaring
delegated acts and implementing acts • committee procedure	gedelegeerde handelingen en uitvoeringshandelingen • comitéprocedure
documentation obligation	registratieverplichting
derogation	afwijking (beperking, uitzondering)
enforcement • administrative fines • administrative penalties • criminal penalties • dissuasive penalties • effective penalties • proportionate penalties	handhaving • administratieve geldboeten • administratieve sancties • juridische sancties • afschrikkende sancties • doeltreffende sancties • evenredige sancties
enterprise	onderneming
European Economic Area (EEA)	Europese Economische Ruimte (EER)

EU types of legal act • decision • directive • opinion • recommendation • regulation	EU types van juridische maatregelen • besluit • richtlijn • advies • aanbeveling • verordening
European Data Protection Board • chair • confidentiality • independence • procedure • reports • secretariat • tasks	Europees Comité voor gegevensbescherming • voorzitter • vertrouwelijkheid • onafhankelijkheid • procedure • rapportage • secretariaat • taken
European Data Protection Supervisor (EDPS)	Europese Toezichthouder voor gegevensbescherming (EDPS)
European Union legal acts on data protection	Unierechtshandelingen inzake gegevensbescherming
exchange of information	uitwisseling van informatie
exemption	uitzondering
explicit consent	uitdrukkelijke toestemming
filing system	bestand
General Data Protection Regulation (GDPR)	algemene verordening gegevensbescherming (AVG)
genetic data	genetische gegevens
governing body	bestuursorgaan
group of undertakings	groepering van ondernemingen
incident response	reactie op inbreuk m.b.t. persoonsgegevens (datalek)
independent supervisory authorities • activity reports • competence • establishment • powers • tasks	onafhankelijke toezichthoudende autoriteiten • activiteitenverslagen • competentie • oprichting • bevoegdheden • taken
Information Security Management System (ISMS)	managementsysteem voor informatiebeveiliging (ISMS)
information society service	diensten van de informatiemaatschappij
international organization	internationale organisatie
Internet of Things (IOT)	Internet der Dingen (IoT)
joint controllers	gezamenlijke verwerkingsverantwoordelijken
judicial remedy	beroep bij de rechter
lawfulness of processing	rechtmatigheid van de verwerking
legal basis	rechtsgrond
legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR recital (40))	dwingende gerechtvaardigde gronden (AVG, artikel 17/1c, 18/1d en 21/1) en gerechtvaardigde grondslag (AVG, overweging (40))
legitimate interest	gerechtvaardigde belangen
liability	aansprakelijkheid
main establishment	hoofdvestiging

material scope	materieel toepassingsgebied
measures based on DPIA results	maatregelen gebaseerd op DPIA resultaten
National Identification Number	nationaal identificatienummer
non-repudiation	niet-afwijzing
notification obligation	kennisgevingsverplichting
opinion of the board	advies van het comité
personal data	persoonsgegevens
personal data breach	inbreuk in verband met persoonsgegevens
personal data relating to criminal convictions and offences	persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten
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	beginselen inzake verwerking van persoonsgegevens (Lit. C AVG, artikel 5) • verantwoordingsplicht • juistheid • vertrouwelijkheid • minimale gegevensverwerking • behoorlijkheid • integriteit • rechtmatigheid • doelbinding • opslagbeperking • transparantie
policy	beleid
policy rule(s)	beleidsregels
prior consultation	voorafgaande raadpleging
privacy	Privacy
privacy analysis	privacy-analyse
privacy officer/chief privacy officer	privacy officer/chief privacy officer
processing	verwerking
processing (of personal data)	verwerken (van persoonsgegevens)
processing agreement	verwerkingsovereenkomst
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	specifieke verwerkingssituaties • gegevensbeschermingsregels van kerken en religieuze verenigingen • arbeidsverhouding • archivering in het algemeen belang • voor wetenschappelijk of historisch onderzoek • voor statistische doeleinden • vrijheid van meningsuiting en van informatie • nationaal identificatienummer • geheimhoudingsplicht • recht van toegang van het publiek tot officiële documenten
processing which does not require identification	verwerking waarvoor identificatie niet is vereist
processor	verwerker
profiling	profilering
proportionality, the principle of	proportionaliteit, het principe van
pseudonymization	pseudonimisering

quality cycle	kwaliteitscyclus
recipient	ontvanger
relevant and reasoned objection	relevant en gemotiveerd bezwaar
repealed	vervangen
representative	vertegenwoordiger
restriction of processing	beperken van de verwerking
retention period	bewaartermijn
right to compensation	recht op schadevergoeding
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	rechten van de betrokkene • geautomatiseerde individuele besluitvorming • overdraagbaarheid van gegevens • informatie en toegang • regelingen • kennisgevingsplicht • rectificatie en wissing • beperking van de verwerking • beperkingen • 'recht op vergetelheid' • recht van bezwaar • transparantie
risk management	risicomanagement
rules of procedure	procedure
security breach (security incident)	inbreuk op de beveiliging (incident)
security of personal data	persoonsgegevensbeveiliging
security of processing	beveiliging van de verwerking
sensitive data	gevoelige gegevens
service provider	serviceprovider
seven principles for privacy by design (Lit. A Chapter 5, paragraph Privacy by design and by default)	de zeven principes van privacy door ontwerp (Lit. A hoofdstuk 5, paragraaf 'Privacy by design and by default')
Social, Mobile, Analytics, Cloud, Things (SMACT)	Social, Mobile, Analytics, Cloud, Things (SMACT)
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	bijzondere categorieën van persoonsgegevens • biometrische gegevens • gegevens over gezondheid, • genetische gegevens, • politieke opvattingen • ras of etnische afkomst • religieuze of levensbeschouwelijke overtuigingen • seksueel gedrag of seksuele gerichtheid • lidmaatschap van een vakbond
subsidiarity, the principle of	subsidiariteit, het principe van
supervisory authority	toezichthoudende autoriteit
supervisory authority concerned	betrokken toezichthoudende autoriteit
suspension of proceedings	schorsing van de procedure
territorial scope	territoriaal toepassingsgebied
third party	derde
threat	(be)dreiging

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	doorgeven van persoonsgegevens aan derde landen of internationale organisaties • adequaatheidsbesluit • passende waarborgen • bindende bedrijfsvoorschriften • afwijkingen • verstrekkingen • internationale samenwerking voor de bescherming van persoonsgegevens
unified communications and collaboration (UCC)	uniforme communicatie en samenwerking (UCC)
vulnerability	kwetsbaarheid

4. Literatuur

Examenliteratuur

De benodigde kennis voor het examen wordt in de volgende literatuur beschreven:

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 editie (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, beschikbaar op 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 beschikbaar op http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

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 beschikbaar op http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Toelichting

De exameneisen zijn gebaseerd op de examenliteratuur. Literatuur C is geen primaire literatuur, omdat de overige examenliteratuur voldoende inhoud bevat over de GDPR. Kandidaten moeten op de hoogte zijn van literatuur C voor zover er door de overige literatuur aan wordt gerefereerd. Literatuur C mag geraadpleegd worden tijdens het examen. Het wordt als appendix bij het digitale examen aangeboden. Breng bij een examen op papier s.v.p. uw eigen exemplaar mee.

Aanvullende literatuur

F. Voorbeeld van Privacy by Design Framework
https://www.privacycompany.eu/files/DPbD_Framework.pdf

Toelichting

De aanvullende literatuur dient alleen ter referentie en het verdiepen van kennis.

Literatuurmatrix

Exameneis	Examenspecificatie	Literatuur
1. Gegevensbeschermingsbeleid		
	1.1 doel van het gegevensbeschermings-/privacybeleid binnen een organisatie	A: Hoofdstuk 16 paragraaf Using policies to demonstrate compliance
	1.2 gegevensbescherming door ontwerp en door standaardinstellingen	A: Hoofdstuk 5 paragraaf Privacy by design and by default
2. Gegevensbescherming beheren en organiseren		
	2.1 fases van het managementsysteem voor gegevensbescherming (DPMS)	A: Hoofdstuk 12 paragraaf Records of processing A: Hoofdstuk 14 introduction + paragraaf Notification B: Hoofdstuk 2, paragraaf 2 DP&P System Phases
	2.2 actieplan voor bewustzijnsvorming over gegevensbescherming	*Nog geen literatuur beschikbaar*
3. Rollen van de verwerkingsverantwoordelijke, verwerker en functionaris voor gegevensbescherming (FG)		
	3.1 rollen van de verwerkingsverantwoordelijke en verwerker	A: Hoofdstuk 12
	3.2 rol en verantwoordelijkheden van een FG	A: Hoofdstuk 2 B: Hoofdstuk 2 paragraaf 2 Phase 4 D: Hoofdstuk 2 paragraaf 1 Mandatory designation D: Hoofdstuk 4 Tasks of the DPO D: Hoofdstuk 5 paragraaf 1 Which organizations must appoint a DPO?
4. Gegevensbeschermingeffectenbeoordeling (DPIA)		
	4.1 criteria for a DPIA	A: Hoofdstuk 5 introduction, paragraaf Privacy Impact Assessments and paragraaf When to conduct a DPIA A: Hoofdstuk 6 paragraaf DPIA's as part of risk management A:"Hoofdstuk 8 paragraaf Objectives and outcomes E: Hoofdstuk 3 DPIA: the Regulation explained

	4.2 stappen van een DPIA	A: Hoofdstuk 5 paragraaf Privacy Impact Assessments A: Hoofdstuk 7 A: Hoofdstuk 8 paragraaf Five key stages in a DPIA and Paragraaf Consultation E: Hoofdstuk 3 DPIA: the Regulation explained
5. Inbreuken in verband met persoonsgegevens, melding van en reactie op inbreuken in verband met persoonsgegevens		
	5.1 vereisten van de AVG over inbreuken in verband met persoonsgegevens	A: Hoofdstuk 3 paragraaf Personal data breaches, Anatomy of a data breach, Sites of attack A: Hoofdstuk 14 paragraaf Notification, Paragraaf Events vs incidents, paragraaf Types of incidents
	5.2 vereisten voor melding	A: Hoofdstuk 14 paragraaf Notification, Paragraaf Key roles in incident management, Paragraaf Respond and paragraaf Follow up

Toelichting

Aan literatuur C, de GDPR, wordt niet in detail gerefereerd.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER