

Preparation guide

Editie 202101

Copyright © EXIN Holding B.V. 2021. All rights reserved.
EXIN® is a registered trademark.

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

Inhoud

1. Overzicht 4
2. Exameneisen 7
3. Begrippenlijst 10
4. Literatuur 15

1. Overzicht

EXIN Privacy & Data Protection Practitioner (PDPP.NL)

Scope

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

Samenvatting

Met de steeds toenemende stroom 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 zowel privacy als gegevensbescherming te reguleren.

De Europese Commisie heeft de Algemene Verordening Gegevensbescherming (AVG) gepubliceerd, wat inhoudt dat vanaf 25 mei 2018 zich moeten houden aan specifieke regels. De EXIN Privacy & Data Protection Practitioner certificering bouwt voort op de onderwerpen van het Foundation examen door zich te richten 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 gegevensbescherming (DPMS).

De nieuwe norm in de ISO/IEC 27000-serie: ISO/IEC 27701:2019 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines is nuttig voor organisaties die willen laten zien dat zij voldoen aan de AVG. Aan de hand van de inhoud van de nieuwe ISO-norm kunnen organisaties hun AVG-verplichtingen voor de verwerking van persoonsgegevens beter nakomen.

De AVG noch de ISO-norm behoren tot de examenliteratuur. Het literatuuroverzicht in hoofdstuk 4 is echter zodanig opgesteld dat hieruit het verband tussen de examenvereisten, de literatuur, de AVG en de norm ISO/IEC 27701:2019 blijkt. Dit is gedaan om een bredere context voor de certificering te bieden.

Context

De certificering EXIN Privacy & Data Protection Practitioner is onderdeel van het certificeringsprogramma EXIN Privacy & 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 analisten en HR-managers.

Certificeringseisen

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

Examendetails

Examenvorm:	Multiple-choicevragen
Aantal vragen:	40
Cesuur:	65% (26/40 vragen)
Open boek:	De GDPR-tekst mag gedurende het examen geraadpleegd worden. Deze tekst is als bijlage beschikbaar in het digitale examen. Voor examens op papier moeten kandidaten hun eigen exemplaar meebrengen.
Notities:	Nee
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.

Indicatie studielast

112 uur (4 ECTS), 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).

Exameneisen	Examenspecificaties	Gewicht
1. Gegevensbeschermingsbeleid		**10%**
	1.1 Het doel van het gegevensbeschermings- en privacybeleid binnen een organisatie	5%
	1.2 Gegevensbescherming door ontwerp en door standaardinstellingen	5%
2. Gegevensbescherming beheren en organiseren		**32,5%**
	2.1 Fasen van het managementsysteem voor gegevensbescherming (DPMS)	32,5%
3. Rollen van de verwerkingsverantwoordelijke, verwerker en functionaris voor gegevensbescherming (FG)		**17,5%**
	3.1 Rollen van de verwerkingsverantwoordelijke en verwerker	10%
	3.2 De rol en verantwoordelijkheden van een FG	7,5%
4. Gegevensbeschermingeffectenbeoordeling (DPIA)		**27,5%**
	4.1 Criteria voor een DPIA	12,5%
	4.2 De stappen van een DPIA	15%
5. Inbreuken in verband met persoonsgegevens, melding van en reactie op inbreuken in verband met persoonsgegevens		**12,5%**
	5.1 Vereisten van de AVG over inbreuken in verband met persoonsgegevens	2,5%
	5.2 Vereisten voor melding	10%
	Totaal	**100%**

Examenspecificaties

1 Gegevensbeschermingsbeleid

1.1 Het doel van het gegevensbeschermings- en privacybeleid binnen een organisatie
De kandidaat kan…
- 1.1.1 uitleggen welk beleid en welke procedures binnen een organisatie nodig zijn om aan de wetgeving inzake gegevensbescherming te voldoen.
- 1.1.2 de inhoud van het beleid uitleggen.

1.2 Gegevensbescherming door ontwerp en door standaardinstellingen
De kandidaat kan…
- 1.2.1 uitleggen wat het concept gegevensbescherming door ontwerp en door standaardinstellingen inhoudt.
- 1.2.2 de zeven principes voor gegevensbescherming door ontwerp en door standaardinstellingen beschrijven.
- 1.2.3 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 laten zien hoe fase 1 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Voorbereiding.
- 2.1.2 laten zien hoe fase 2 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Organisatie.
- 2.1.3 laten zien hoe fase 3 van het DPMS kan worden toegepast: Gegevensbescherming en privacy: Ontwikkeling en implementatie.
- 2.1.4 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.

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 naleven.
- 3.1.2 de verantwoordelijkheden van de verwerker naleven.
- 3.1.3 de relatie tussen de verwerkingsverantwoordelijke en de verwerker uitleggen voor een specifieke situatie.

3.2 De rol en verantwoordelijkheden van een FG
De kandidaat kan…
- 3.2.1 uitleggen wanneer de AVG het aanstellen van een FG verplicht stelt.
- 3.2.2 de rol van de FG naleven.
- 3.2.3 de positie van de FG ten opzichte van de toezichthoudende autoriteit uitleggen.

4 Gegevensbeschermingseffectbeoordeling (DPIA)

4.1 Criteria voor een DPIA
De kandidaat kan…
- 4.1.1 de criteria voor het uitvoeren van een DPIA toepassen.
- 4.1.2 de doelen en uitkomsten van een DPIA beschrijven.

4.2 De stappen van een DPIA
De kandidaat kan…
- 4.2.1 de stappen van een DPIA beschrijven.
- 4.2.2 een DPIA uitvoeren 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 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 melden.

5.2.2 de betrokkenen op de hoogte brengen van de inbreuk in verband met persoonsgegevens.

5.2.3 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.

Engels	**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 (BCR)	bindende bedrijfsvoorschriften (BCR)
biometric data	biometrische gegevens
bring your own device (BYOD)	bring your own device (BYOD)
certification	certificering
certification bodies	certificeringsorganen
cloud computing	cloud computing
codes of conduct	gedragscodes
collection of personal data (verb.)	verzamelen van persoonsgegevens
commission reports	commissieverslagen
complaint	klacht
compliance	voldoen (aan)
consent • child's consent • conditions for consent • explicit consent	toestemming • toestemming van kinderen • voorwaarden voor toestemming • uitdrukkelijke toestemming
consistency	coherentie
consistency mechanism	coherentiemechanisme
constitution	grondwet
contract	overeenkomst
controller	verwerkingsverantwoordelijke
cross-border processing	grensoverschrijdende verwerking
data accuracy	juistheid van gegevens
data breach	inbreuk in verband met gegevens
data classification system	systeem voor gegevensclassificatie
data concerning health	gegevens over gezondheid
data lifecycle management (DLM)	data lifecycle management (DLM)
data mapping	gegevensstromen in kaart brengen
data portability	gegevensoverdraagbaarheid
data protection	gegevensbescherming

(data privacy) breach response plan / data privacy incident response plan	reactieplan inbreuk in verband met persoonsgegevens / reactieplan privacy-inbreuk
data protection authority (DPA)	toezichthoudende autoriteit *In Nederland is dit de 'Autoriteit Persoonsgegevens' (AP) en in België de '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)	gegevensbeschermingseffectbeoordeling (DPIA)
Data Protection Management System (DPMS)	managementsysteem voor 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
filing system	bestand
General Data Protection Regulation (GDPR)	Algemene Verordening Gegevensbescherming (AVG)
genetic data	genetische gegevens
governing body	bestuursorgaan
group of undertakings	concern
incident response	reactie op inbreuk in verband met persoonsgegevens
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	dienst van de informatiemaatschappij
international organization	internationale organisatie
Internet of Things (IOT)	Internet of Things (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
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 (GDPR, Article 5) • accountability • accuracy • confidentiality • data minimization • fairness • integrity • lawfulness • purpose limitation • storage limitation • transparency	beginselen inzake verwerking van persoonsgegevens (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	intrekken
representative	vertegenwoordiger
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 inzage • regelingen • kennisgevingsplicht • rectificatie en gegevenswissing • 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 (Literature: A, Chapter 5, paragraph 'Privacy by Design and by Default')	de zeven principes van privacy door ontwerp (Literatuur: 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 overtuiging • 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 • derogations • disclosures • international protection of personal data	doorgeven van persoonsgegevens aan derde landen of internationale organisaties • adequaatheidsbesluit • passende waarborgen • 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 (tweede editie, 2017)
ISBN 978-1-84928-9450 (hardcopy)
ISBN 978-1-84928-9474 (e-book)

B. Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide – Vol. I
bookboon.com (eerste editie, 2016)
ISBN 978-87-403-1540-0

Aanvullende literatuur

C. Europese Commissie
Algemene verordening gegevensbescherming (AVG) (Verordening (EU) 2016/679)
Verordening van het Europees parlement en de Raad van de Europese.
Brussel, 27 April 2016, beschikbaar op http://eur-lex.europa.eu
Nederlandse versie:
https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL
Engelse versie (GDPR):
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

D. Groep Gegevensbescherming Artikel 29
Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), wp 243rev.01
13 december 2016, Nederlandse versie beschikbaar op:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243rev01_nl.pdf
Engelse versie:
http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=612048

E. Groep Gegevensbescherming Artikel 29
Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, wp248
4 april 2017, Nederlandse versie beschikbaar op:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf
Engelse versie:
http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236

F. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines
Switzerland, ISO/IEC, 2019
https://www.iso.org/home.html

Toelichting

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

De tekst van de AVG (bron C) is geen verplichte examenliteratuur, omdat de examenliteratuur voldoende kennis van de AVG biedt. Kandidaten moeten wel bekend zijn met de referenties die de literatuur maakt naar de AVG.

Literatuurmatrix

Exameneisen	Examen-specificaties	Literatuur-referentie	AVG-referentie	ISO/IEC 27701 referentie
1. Gegevensbeschermingsbeleid				
	1.1 Het doel van het gegevensbeschermings- en privacybeleid binnen een organisatie	A, Hoofdstuk 1, Hoofdstuk 16	*geen referentie*	*geen referentie*
	1.2 Gegevensbescherming door ontwerp en door standaardinstellingen	A, Hoofdstuk 5	Artikel 25	Sectie B.8.4, Subclausule 6.11.2.1, Subclausule 6.11.2.5, Subclausule 7.4.2
2. Gegevensbescherming beheren en organiseren				
	2.1 Fasen van het managementsysteem voor gegevensbescherming (DPMS)	A, Hoofdstuk 12 Hoofdstuk 14 B, Hoofdstuk 2	*geen referentie*	*geen referentie*
3. Rollen van de verwerkingsverantwoordelijke, verwerker en functionaris voor gegevensbescherming (FG)				
	3.1 Rollen van de verwerkingsverantwoordelijke en verwerker	A, Hoofdstuk 12	Artikel 24, Artikel 26, Artikel 27, Artikel 28, Artikel 29	Subclausule 5.2.1, Subclausule 6.3.1.1, Subclausule 6.12.1.2, Subclausule 6.15.1.1, Subclausule 7.2.6, Subclausule 7.2.7, Subclausule 8.2.1, Subclausule 8.2.4, Subclausule 8.2.5, Subclausule 8.5.4, Subclausule 8.5.6, Subclausule 8.5.7, Subclausule 8.5.8
	3.2 De rol en verantwoordelijk-heden van een FG	A, Hoofdstuk 2	Artikel 37, Artikel 38, Artikel 39	Subclausule 6.3.1.1, Subclausule 6.4.2.2, Subclausule 6.10.2.4

4. Gegevensbeschermingeffectenbeoordeling (DPIA)				
	4.1 Criteria voor een DPIA	A, Hoofdstuk 5, Hoofdstuk 6, Hoofdstuk 7, Hoofdstuk 8	Artikel 35	Subclausule 5.2.2, Subclausule 7.2.5, Subclausule 8.2.1
	4.2 De stappen van een DPIA	A, Hoofdstuk 5, Hoofdstuk 7, Hoofdstuk 8	*geen referentie*	Subclausule 5.2.2, Subclausule 7.2.5, Subclausule 8.2.1
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, Hoofdstuk 14	Artikel 4(12), Artikel 33, Artikel 34	Subclausule 6.13.1.1, Subclausule 6.13.1.5
	5.2 Vereisten voor melding	A, Hoofdstuk 14	Artikel 33, Artikel 34	Subclausule 6.13.1.1, Subclausule 6.13.1.5



Contact EXIN

www.exin.com