Preparation guide

Editie 202308

Inhoud

1. Overzicht

EXIN Privacy & Data Protection Foundation (PDPF.NL)

Scope

EXIN Privacy & Data Protection Foundation (PDPF) is een certificering die de kennis en het begrip van een professional bevestigt van de bescherming van persoonsgegevens en van de EU-regels en -voorschriften met betrekking tot gegevensbescherming.

Samenvatting

Overal waar persoonsgegevens worden verzameld, opgeslagen, gebruikt en uiteindelijk verwijderd of vernietigd, kan privacy in het geding zijn Met de Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie (EU) wil de Raad van de EU de gegevensbescherming voor alle personen in de EU versterken en harmoniseren. Deze verordening is van invloed op elke organisatie die, waar ook ter wereld, persoonsgegevens verwerkt van personen die zich binnen de EU bevinden. EXIN Privacy and Data Protection Foundation behandelt de belangrijkste onderwerpen die verband houden met de AVG.

De nieuwe norm in de ISO/IEC 27000-serie: ISO/IEC 27701:2019 Beveiligingstechnieken – uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor het beheer van privacygegevens – Vereisten en richtlijnen 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 Foundation is onderdeel van het certificeringsprogramma EXIN Privacy & Data Protection.

Doelgroep

Alle medewerkers die inzicht moeten hebben in gegevensbescherming en de Europese wettelijke vereisten zoals gedefinieerd in de AVG. Deze certificering is specifiek gericht op:

- functionarissen voor gegevensbescherming (FG's)
- nalevingsfunctionarissen
- beveiligingsfunctionarissen
- HR-personeel
- proces- en projectmanagers

Certificeringseisen

- Met goed gevolg afleggen van het examen EXIN Privacy & Data Protection Foundation.

Examendetails

Examenvorm:	Multiple-choicevragen
Aantal vragen:	40
Cesuur:	65% (26/40 vragen)
Open boek:	Nee
Notities:	Nee
Elektronische hulpmiddelen toegestaan:	Nee
Examenduur:	60 minuten

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

Bloom level

De certificering EXIN Privacy & Data Protection Foundation toetst kandidaten op Bloom Levels 1 en 2 volgens Bloom's Revised Taxonomy:

- Bloom level 1: Onthouden – Op dit niveau kunnen kandidaten zich de geleerde stof herinneren. Ze kunnen herkennen, beschrijven en benoemen.
- 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.

Training

Contacturen

Het aangeraden aantal contacturen tijdens de training is 14. Dit omvat groepsopdrachten, voorbereiding op het examen en korte pauzes. Dit aantal uren is exclusief lunchpauzes, huiswerk en het examen.

Indicatie studielast

56 uur (2 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. Grondbeginselen en wetgeving op het gebied van privacy en gegevensbescherming		**47,5%**
	1.1 Definities	7,5%
	1.2 Persoonsgegevens	17,5%
	1.3 Gerechtvaardigde grondslagen en doelbinding	5%
	1.4 Aanvullende vereisten voor gerechtvaardigde verwerking van persoonsgegevens	5%
	1.5 Rechten van betrokkenen	2,5%
	1.6 Inbreuk in verband met persoonsgegevens en hieraan gerelateerde procedures	10%
2. Organiseren van gegevensbescherming		**35%**
	2.1 Het belang van gegevensbescherming voor de organisatie	12,5%
	2.2 Toezichthoudende autoriteit	7,5%
	2.3 Doorgiften van persoonsgegevens aan derde landen	7,5%
	2.4 Bindende bedrijfsvoorschriften (BCR) en gegevensbescherming in overeenkomsten	7,5%
3. Gegevensbescherming in praktijk		**17,5%**
	3.1 Gegevensbescherming door ontwerp en door standaardinstellingen voor informatiebeveiliging	5%
	3.2 Gegevensbeschermingseffectbeoordeling (DPIA)	5%
	3.3 Gebruik van persoonsgegevens	7,5%
	Totaal	**100%**

Examenspecificaties

1 Grondbeginselen en wetgeving op het gebied van privacy en gegevensbescherming

1.1 Definities

De kandidaat kan…

1.1.1 een definitie geven van privacy.

1.1.2 het verband leggen tussen privacy, persoonsgegevens en gegevensbescherming.

1.1.3 de context van het Unierecht en lidstatelijk recht beschrijven.

1.2 Persoonsgegevens

De kandidaat kan…

1.2.1 een definitie geven van persoonsgegevens volgens de AVG.

1.2.2 onderscheid maken tussen persoonsgegevens en bijzondere categorieën van gegevens, zoals gevoelige persoonsgegevens.

1.2.3 de rechten van een betrokkene met betrekking tot diens persoonsgegevens beschrijven.

1.2.4 beschrijven wanneer verwerking van persoonsgegevens valt binnen het toepassingsgebied van de AVG.

1.2.5 de rollen, verantwoordelijkheden en belanghebbenden volgens de AVG benoemen.

1.3 Gerechtvaardigde grondslagen en doelbinding

De kandidaat kan…

1.3.1 de zes gerechtvaardigde grondslagen voor verwerking benoemen.

1.3.2 het begrip doelbinding beschrijven.

1.3.3 proportionaliteit en subsidiariteit beschrijven.

1.4 Aanvullende vereisten voor gerechtvaardigde verwerking van persoonsgegevens

De kandidaat kan…

1.4.1 de vereisten voor rechtmatige gegevensverwerking beschrijven.

1.4.2 het doel van gegevensverwerking beschrijven.

1.4.3 de beginselen met betrekking tot de verwerking van persoonsgegevens beschrijven.

1.5 Rechten van betrokkenen

De kandidaat kan…

1.5.1 het recht op overdraagbaarheid van gegevens en het recht van inzage beschrijven.

1.5.2 het recht op vergetelheid beschrijven.

1.6 Inbreuk in verband met persoonsgegevens en hieraan gerelateerde procedures

De kandidaat kan…

1.6.1 het begrip ‘inbreuk in verband met persoonsgegevens’ beschrijven.

1.6.2 de procedures uitleggen die moeten worden gevolgd wanneer er zich een inbreuk in verband met persoonsgegevens voordoet.

1.6.3 voorbeelden geven van categorieën van inbreuk in verband met persoonsgegevens.

1.6.4 het verschil beschrijven tussen een inbreuk op de beveiliging (incident) en een inbreuk in verband met persoonsgegevens.

1.6.5 relevante belanghebbenden benoemen die op de hoogte moeten worden gesteld in geval van een inbreuk in verband met persoonsgegevens.

2 Organiseren van gegevensbescherming

2.1 Het belang van gegevensbescherming voor de organisatie

De kandidaat kan…

2.1.1 de verschillende soorten administraties benoemen (AVG, Artikel 28 en Artikel 30).

2.1.2 aangeven welke activiteiten vereist zijn om te voldoen aan de AVG.

2.1.3 de begrippen gegevensbescherming door ontwerp en door standaardinstellingen omschrijven.

2.1.4 voorbeelden geven van inbreuken in verband met persoonsgegevens.

2.1.5 de kennisgevingsplicht inzake inbreuk in verband met persoonsgegevens beschrijven zoals vastgelegd in de AVG.

2.1.6 handhaving van de regels door het opleggen van sancties beschrijven, inclusief administratieve geldboetes.

2.2 Toezichthoudende autoriteit

De kandidaat kan…

2.2.1 de algemene verantwoordelijkheden van een toezichthoudende autoriteit beschrijven.

2.2.2 de rol en verantwoordelijkheden van een toezichthoudende autoriteit beschrijven met betrekking tot inbreuken in verband met persoonsgegevens.

2.2.3 beschrijven hoe een toezichthoudende autoriteit bijdraagt aan de toepassing van de AVG.

2.3 Doorgiften van persoonsgegevens aan derde landen

De kandidaat kan…

2.3.1 de voorschriften beschrijven die van toepassing zijn op het doorgeven van persoonsgegevens binnen de EER.

2.3.2 de voorschriften beschrijven die van toepassing zijn op het doorgeven van persoonsgegevens buiten de EER.

2.3.3 de voorschriften beschrijven die van toepassing zijn op het doorgeven van persoonsgegevens tussen de EER en de VS.

2.4 Bindende bedrijfsvoorschriften (BCR) en gegevensbescherming in overeenkomsten

De kandidaat kan…

2.4.1 het begrip ‘bindende bedrijfsvoorschriften’ (BCR) beschrijven.

2.4.2 beschrijven hoe gegevensbescherming in overeenkomsten tussen de verwerkingsverantwoordelijke en de verwerker wordt geformaliseerd.

2.4.3 de bepalingen van een dergelijke overeenkomst beschrijven.

3 Gegevensbescherming in praktijk

3.1 Gegevensbescherming door ontwerp en door standaardinstellingen voor informatiebeveiliging

De kandidaat kan…

3.1.1 de voordelen beschrijven van gegevensbescherming door ontwerp en door standaardinstellingen.

3.1.2 de zeven beginselen van gegevensbescherming door ontwerp beschrijven.

3.2 Gegevensbeschermingseffectbeoordeling (DPIA)

De kandidaat kan…

3.2.1 globaal omschrijven wat in een DPIA aan bod komt en wanneer een DPIA moet worden uitgevoerd.

3.2.2 de acht doelstellingen van een DPIA noemen.

3.2.3 de onderwerpen van een DPIA-verslag benoemen.

3.3 Gebruik van persoonsgegevens

De kandidaat kan…

3.3.1 het doel van data lifecycle management (DLM) beschrijven.

3.3.2 gegevensbehoud en minimale gegevensverwerking uitleggen.

3.3.3 beschrijven wat een cookie is en wat het doel ervan is.

3.3.4 het recht van bezwaar tegen de verwerking van persoonsgegevens voor direct marketing beschrijven, inclusief profilering.

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
authenticity	authenticiteit
availability	beschikbaarheid
awareness	bewustzijn, besef
benchmark	benchmark (vergelijken / vergelijking met een standaard)
binding corporate rules (BCR)	bindende bedrijfsvoorschriften (BCR)
certification / certification bodies	certificering / certificeringsorganen
collecting of personal data	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 aan toestemming • uitdrukkelijke toestemming
consistency / consistency mechanism	coherentie / coherentiemechanisme
constitution	grondwet
controller	verwerkingsverantwoordelijke
cross-border processing	grensoverschrijdende verwerking
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 privacy) breach response plan	reactieplan inbreuk in verband met persoonsgegevens
Data Privacy Framework	Data Privacy Framework[1]
data protection	gegevensbescherming
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)

[1] In juli 2023 heeft de EU een adequaatheidsbesluit genomen ten aanzien van het EU-VS Data Privacy Framework

data protection officer (DPO) • designation • position • tasks	functionaris voor gegevensbescherming (FG) • aanwijzing • positie • taken
data subject	betrokkene
data transfer	doorgeven van persoonsgegevens
declaration of consent	toestemmingsverklaring
delegated acts and implementing acts • committee procedure	gedelegeerde handelingen en uitvoeringshandelingen • comitéprocedure
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)
governing body	bestuursorgaan
group of undertakings	concern
information society service	dienst van de informatiemaatschappij
international organization	internationale organisatie
joint controllers	gezamenlijke verwerkingsverantwoordelijken
judicial remedy	beroep bij de rechter
lawfulness of processing	rechtmatigheid van de verwerking
legal basis	rechtsgrond
legitimate basis (GDPR Recital 40)	gerechtvaardigde grondslag (AVG overweging 40)
legitimate grounds (GDPR Article 17/1c, Article 18/1d, Article 21/1)	gerechtvaardigde gronden (AVG, artikel 17/1c, 18/1d en 21/1); rechtsgrond

legitimate interest	gerechtvaardigde belangen
liability	aansprakelijkheid
main establishment	hoofdvestiging
material scope	materieel toepassingsgebied
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
prior consultation	voorafgaande raadpleging
privacy	privacy
privacy analysis	privacy-analyse
privacy officer / chief privacy officer	privacy officer / chief privacy officer
processing (of personal data)	verwerken (van persoonsgegevens)
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	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
recipient	ontvanger
relevant and reasoned objection	relevant en gemotiveerd bezwaar
representative	vertegenwoordiger
retention period	bewaartermijn

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
rules of procedure	procedure
security breach	inbreuk op de beveiliging
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	de zeven principes van privacy door ontwerp
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
vulnerability	kwetsbaarheid

4. Literatuur

Examenliteratuur

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

A. L. Besemer
Privacy and Data Protection based on the GDPR
Van Haren Publishing, 2020
ISBN: 978 94 018 0676 3 (gedrukt boek)
ISBN: 978 94 018 0677 0 (e-book)
ISBN: 978 94 018 0678 7 (e-pub)

Aanvullende literatuur

B. European Commission
General Data Protection Regulation (GDPR) Regulation EU 2016/679
Regulation of the European Parliament and the Council of the European Union.
Brussel, 6 April 2016
Gratis te downloaden van: http://eur-lex.europa.eu (pdf) of https://gdpr-info.eu/ (html)

C. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

D. A. Calder
EU GDPR, A pocket guide
IT Governance Publishing
ISBN 978-1-84928-855-2 (gedrukt boek)
ISBN 978-1-84928-857-6 (e-book)

Toelichting

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

De AVG tekst (literatuur B) behoort niet tot de primaire examenliteratuur, omdat de andere literatuur voldoende informatie bevat over de AVG. Kandidaten moeten wel bekend zijn met de verwijzingen naar de AVG die gemaakt worden in de examenliteratuur.

Literatuurmatrix

Exameneisen	Examenspecificaties	Literatuur-referentie	AVG-referentie	ISO/IEC 27701-referentie
1. Grondbeginselen en wetgeving op het gebied van privacy en gegevensbescherming				
	1.1 Definities	A, Hoofdstuk 1	Overweging 1, 2 & Artikel 96-99	*geen referentie*
	1.2 Persoonsgegevens	A, Hoofdstuk 1, Hoofdstuk 2, Hoofdstuk 3, Hoofdstuk 4, Hoofdstuk 5	Artikel 4.1(a), Artikel 9.1, Artikel 17, Artikel 4.10	Subclausule 7.2.2, Subclausule 7.3.6
	1.3 Gerechtvaardigde grondslagen en doelbinding	A, Hoofdstuk 3, Hoofdstuk 4	Artikel 6.1, Artikel 24	Subclausule 7.2.2
	1.4 Aanvullende vereisten voor gerechtvaardigde verwerking van persoonsgegevens	A, Hoofdstuk 3	Artikel 25, Artikel 27-32, Artikel 5	Subclausule 5.2.1. *Aan Artikel 5 wordt in het hele document gerefereerd.*
	1.5 Rechten van betrokkenen	A, Hoofdstuk 5	Artikel 15, Artikel 16, Artikel 17, Artikel 18, Artikel 20, Artikel 21, Artikel 22	Subclausule 7.2.2, Subclausule 7.3.2, Subclausule 7.3.6, Subclausule 7.3.9, Subclausule 7.3.10, Subclausule 7.5.1
	1.6 Inbreuk in verband met persoonsgegevens en hieraan gerelateerde procedures	A, Hoofdstuk 11	Artikel 4(12), Artikel 33, Artikel 34	Subclausule 6.13.1.5
2. Organiseren van gegevensbescherming				
	2.1 Het belang van gegevensbescherming voor de organisatie	A, Hoofdstuk 2, Hoofdstuk 4, Hoofdstuk 10, Hoofdstuk 11, Hoofdstuk 12	Artikel 7, Artikel 8, Artikel 13, Artikel 25(1), Artikel 30, Artikel 83	Subclausule 6.11.2.1, Subclausule 6.11.2.5, Subclausule 7.2.3, Subclausule 7.2.4, Subclausule 7.2.5, Subclausule 7.2.8, Subclausule 7.3.2, Subclausule 7.3.6, Subclausule 7.3.10, Subclausule 7.5, Subclausule 8.2.6, Subclausule 8.5.2, Subclausule 8.5.3
	2.2 Toezichthoudende autoriteit	A, Hoofdstuk 12	Artikel 33, Artikel 34, Artikel 36	Subclausule 5.2.2, Subclausule 6.13.1.1, Subclausule 6.13.1.5, Subclausule 7.2.5
	2.3 Doorgiften van persoonsgegevens aan derde landen	A, Hoofdstuk 8, Hoofdstuk 9	Artikel 29, Artikel 30, Artikel 45	Subclausule 7.2.8, Subclausule 7.5, Subclausule 8.2.2, Subclausule 8.2.6

	2.4 Bindende bedrijfsvoorschriften (BCR) en gegevensbescherming in overeenkomsten	A, Hoofdstuk 2, Hoofdstuk 9	Artikel 24, Artikel 28, Artikel 47	Subclausule 5.2.1, Subclausule 6.12.1.2, Subclausule 7.2.6, Subclausule 7.2.8, Subclausule 7.5.1, Subclausule 8.5
3. Gegevensbescherming in praktijk				
	3.1 Gegevensbescherming door ontwerp en door standaardinstellingen voor informatiebeveiliging	A, Hoofdstuk 2	Artikel 25	Sectie B.8.4, Subclausule 6.11.2.1, Subclausule 6.11.2.5, Subclausule 7.4.2
	3.2 Gegevensbeschermings-effectbeoordeling (DPIA)	A, Hoofdstuk 10	Artikel 35	Subclausule 5.2.2, Subclausule 7.2.5, Subclausule 8.2.1
	3.3 Gebruik van persoonsgegevens	A, Hoofdstuk 3, Hoofdstuk 5, Hoofdstuk 6, Hoofdstuk 7	*geen referentie*	Sectie B.8.2.3

Contact EXIN

www.exin.com