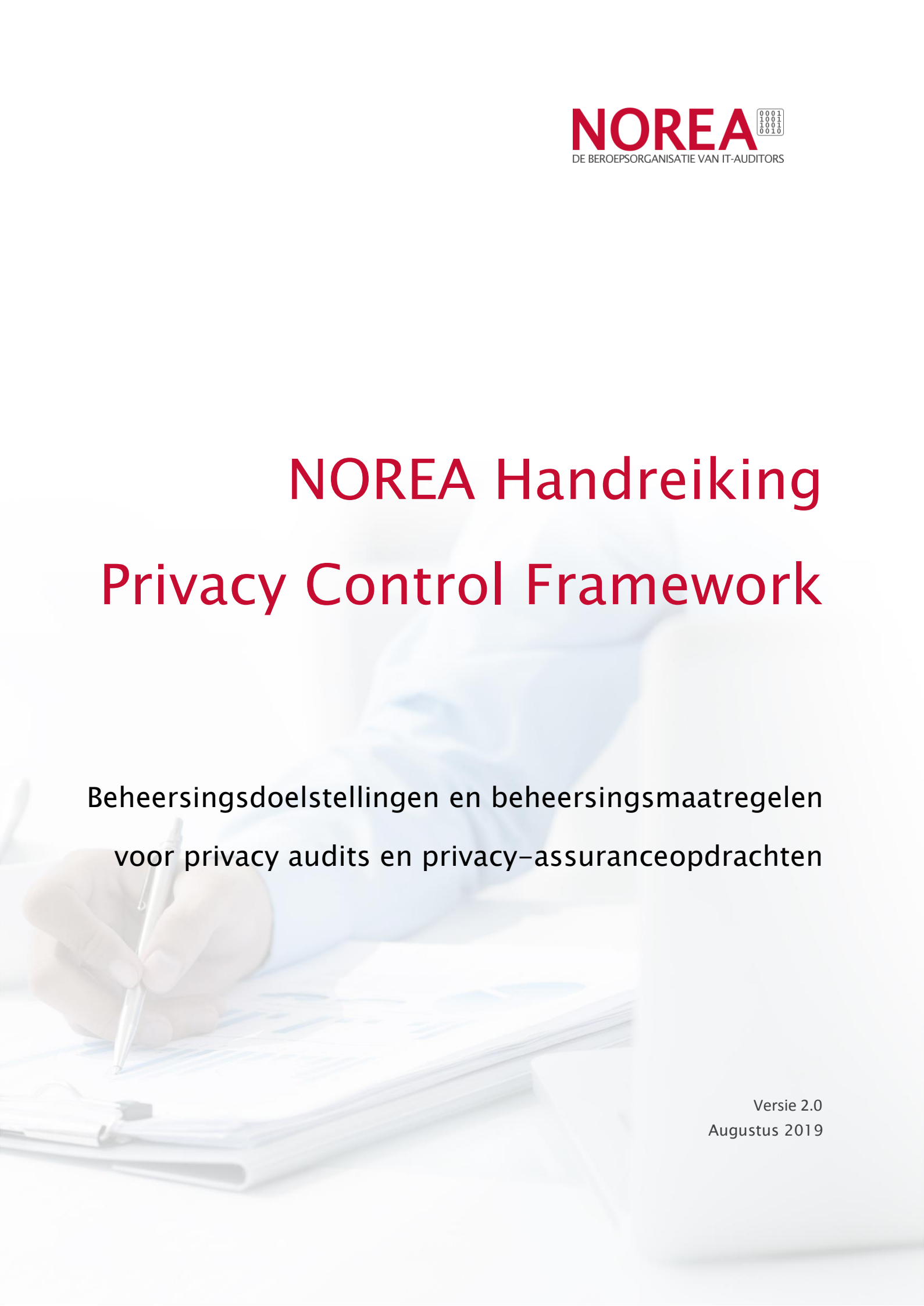
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Handreiking

Privacy Control Framework

Beheersingsdoelstellingen en beheersingsmaatregelen voor privacy audits en privacy-assuranceopdrachten



Versie 2.0
Augustus 2019

Verantwoording

Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en is ontwikkeld om Nederlandse gekwalificeerde IT-auditors (Register IT-auditors, RE's) handvatten te bieden om een assurancerapport op te stellen in lijn met de Europese Algemene Verordening Gegevensbescherming (AVG) en relevante standaarden voor assuranceopdrachten.

Deelnemers werkgroep

De volgende personen hebben namens de NOREA Kennisgroep Privacy en de Werkgroep Privacy Control Framework een bijdrage aan deze handreiking geleverd:

drs. Jaap Boukens RE RA, Jeroen Caron RE MSc CIPP/E, ir. Jan de Heer RE, Maurice Koetsier MSc RE CIPP/E CIPM, Henk van der Linde RA, mr. Winfried Nanninga RE CIA MMC, ir. Ali Ougajou RE, drs. Ed Ridderbeekx RE CISA CIPP/E, ir. Elisabeth Lekkerkerker-Smit RE, Maurice Steffin RC CIPP/E CIPM

Coördinatie en redactie

Versie 1.0: ir. Jan de Heer RE, drs. Ed Ridderbeekx RE CISA CIPP/E
Versie 2.0: drs. Ed Ridderbeekx RE CISA CIPP/E

Postbus 7984, 1008 AD Amsterdam
telefoon: 020-3010380
e-mail: norea@norea.nl www.norea.nl

Versiebeheer		
Versie	Datum	Wijzigingen
1.0	mei 2018	
2.0	augustus 2019	Zie paragraaf 10 in Deel 1 van dit document

Inhoudsopgave

Deel 1 – Introductie

1. Inleiding

In dit document wordt het Privacy Control Framework (hierna: 'PCF') uiteengezet dat is ontwikkeld door NOREA (de Nederlandse beroepsorganisatie van gekwalificeerde IT-auditors / Nederlandse Orde van Register EDP-auditors).

2. Doelstellingen van het Privacy Control Framework

Het primaire doel van het PCF is het bieden van ondersteuning aan (audit)professionals bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald. Het PCF kan worden gebruikt als startpunt voor privacyaudits op maat. Het PCF bevat de voorgeschreven beheersingsdoelstellingen en voorbeelden van maatregelen voor privacyopdrachten op basis van de NOREA Richtlijn 3000. Het PCF kan eveneens worden gebruikt om invulling te geven aan het privacy-deel van een SOC 2® assurance rapport voor een entiteit die moet voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

Het PCF kan daarnaast door entiteiten worden gebruikt om vast te stellen of de maatregelen ten aanzien van privacybescherming adequaat zijn, of om te bepalen in hoeverre de huidige maatregelen dienen te worden aangepast om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG).

3. Opbouw van het Privacy Control Framework

Het PCF is gebaseerd op een informatielevenscyclusmodel, waarbij de volgende 'best practice' raamwerken in ogenschouw werden genomen:

1. GAPP – gepubliceerd door de AICPA/CICA;[1]
2. NIST SP800-R53 Privacy Control Catalog;[2]
3. NOREA Raamwerk Privacy Audit;[3]
4. EuroPriSe raamwerk.[4]

In bijlage 2 wordt de informatielevenscyclus verder toegelicht. Voor elke fase is bepaald welke privacyonderwerpen van toepassing zijn. Deze onderwerpen worden weergegeven door middel van een afkorting van drie letters (32 in totaal). Elk privacyonderwerp is gekoppeld aan een beheersingsdoelstelling en deze is vervolgens vertaald naar een aantal beheersingsmaatregelen die dienen te worden

[1] An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009.

[2] Security and Privacy Controls for Federal Information, Systems and Organizations, NIST SP800-R53 Privacy Control Catalog, 2013

[3] Het NOREA Raamwerk Privacy Audit, 2005, Addendum Norea Privacy Audit bij Richtlijn 3600n, 2017

[4] European Privacy Seal EuroPriSe, 2008

geëvalueerd (95 in totaal). Deel 2 biedt een overzicht van de privacyonderwerpen en de hieraan gerelateerde beheersingsdoelstellingen. Deel 3 bevat een gedetailleerde lijst met de beheersingsmaatregelen per onderwerp.

4. Het Privacy Control Framework en de AVG

De beheersingsdoelstellingen en de voorbeelden van maatregelen in het PCF sluiten nauw aan bij en zijn gekoppeld aan 13 kernelementen van de AVG. De kernelementen zijn geselecteerd op basis van een deskundig oordeel en de onderwerpen in het document 'In 10 stappen voorbereid op de AVG' van de Autoriteit Persoonsgegevens. Wanneer een entiteit de volledige set PCF-criteria hanteert, dient men deze hoofdonderwerpen van de AVG te behandelen en maatregelen te treffen om de van toepassing zijnde wettelijk verplichte doelstellingen te behalen.

Met de implementatie en uitvoering van de maatregelen kan met een redelijke mate van zekerheid gewaarborgd worden dat de beheersingsdoelstelling waartoe die maatregelen behoren wordt behaald. Hoewel de beheersingsdoelstellingen en -maatregelen in het PCF aansluiten op de beginselen van de AVG, biedt het toepassen van het PCF niet de garantie dat ook volledig aan de vereisten uit de AVG wordt voldaan. De AVG is een veelomvattende wet die tal van gedetailleerde vereisten voor specifieke situaties bevat. Met het oog op de praktische toepasbaarheid van het document worden deze vereisten niet allemaal in het PCF behandeld.

Professionals die de privacymaatregelen van een entiteit beoordelen (bijvoorbeeld door via een gap-analyse vast te stellen of de entiteit aan de eisen van de AVG voldoet) wordt aangeraden aanvullende bronnen te gebruiken bij de identificatie en naleving van de specifieke wettelijke vereisten (zoals de Uitvoeringswet AVG) en gezaghebbende leidraden (zoals van de European Data Protection Board, EDPB) die op de betreffende entiteit van toepassing zijn.

In bijlage 1 wordt de relatie tussen het PCF en de AVG weergegeven.

5. Gebruik van het Privacy Control Framework

De manier waarop het PCF in de praktijk wordt gebruikt, is afhankelijk van de doelstellingen van de gebruiker. Over het algemeen worden drie soorten gebruikers onderscheiden:

a. De IT-auditor die de privacymaatregelen van een entiteit en het behalen van privacydoelstellingen beoordeelt, met als doel de mate van privacybescherming of compliance met de AVG te bepalen;

b. De IT-auditor die een privacy-assuranceopdracht uitvoert op basis van NOREA Richtlijn 3000, of een assuranceopdracht gebaseerd op SOC 2 in een entiteit waar het wetgevingskader van de AVG van toepassing is. Daarnaast gebruikt een IT-auditor het PCF als de assuranceopdracht volgens Richtlijn 3000 wordt uitgevoerd in het kader van het verlenen van een Privacy Audit Proof® keurmerk;

c. Andere professionals (zoals risicomanagers, functionarissen voor gegevensbescherming en -beveiliging, en privacymedewerkers) die de mate van privacybescherming of compliance met de AVG van een entiteit wensen te beoordelen (geen audit).

Uitgangspunt is dat de scope van elk van de beoordelingen of opdrachten zoals hierboven genoemd zal worden geformuleerd als een duidelijk omschreven, specifieke en risicogebaseerde (verzameling van) verwerking(en) van persoonsgegevens door de entiteit.

Het PCF geeft voor iedere beheersingsmaatregel aan of die van toepassing is voor een entiteit die optreedt als verwerkingsverantwoordelijke, als verwerker, of als beide. Dit is aangegeven met de letters 'VV' en 'V' in een separate kolom in Deel 3. Het wordt aanbevolen dit te zien in relatie tot de scope van een audit- of assuranceopdracht. Als een entiteit wordt aangemerkt als verwerkingsverantwoordelijke of verwerker voor minimaal één van de verwerkingen in scope, dan zijn de beheersmaatregelen aangeduid met 'VV' respectievelijk 'V' van toepassing.

Beoordeling privacybeheersingsmaatregelen

Bij de beoordeling van de privacybeheersingsmaatregelen kan de IT-auditor het PCF gebruiken als een algemeen toetsingskader en dit aanpassen aan scope van de beoordeling. Het is daarbij goed om eerst de privacyonderwerpen en de hieraan gerelateerde beheersingsdoelstellingen in deel 2 van het PCF door te nemen en daarna een selectie te maken op basis van de scope van de opdracht. Vervolgens kan voor de geselecteerde onderwerpen en doelstellingen worden bepaald welke beheersingsmaatregelen uit deel 3 dienen te worden beoordeeld. Het is tot slot aan de IT-auditor om de beheersingsmaatregelen zodanig te wijzigen of aan te scherpen dat deze zo goed mogelijk zijn afgestemd op de scope en het doel van de opdracht.

Assuranceopdrachten

In het geval van assuranceopdrachten kan het PCF als basis dienen voor de criteria die op grond van de NOREA Richtlijn 3000 moeten worden opgenomen in het assurancerapport. Gebruik van het PCF is verplicht als de assuranceopdracht volgens Richtlijn 3000 wordt uitgevoerd met als doel het uitgeven van een Privacy Audit Proof-keurmerk. Het PCF kan tevens worden gebruikt om invulling te geven aan het privacy-deel van een SOC 2 assurancerapport in een entiteit die moet voldoen aan de AVG (zie ook paragraaf 6 hieronder).

Een IT-auditor kan daarbij alle onderwerpen en beheersingsdoelstellingen in deel 2 als uitgangspunt nemen en deze gebruiken als beheersingsraamwerk in het assurancerapport. De IT-auditor kiest vervolgens in deel 3 zorgvuldig de beheersingsmaatregelen die van toepassing zijn en waarmee de entiteit de beheersingsdoelstellingen kan realiseren. De beheersingsmaatregelen in deel 3 zijn voorbeelden, het is de verantwoordelijkheid van de entiteit om ze, waar nodig, aan de hand van de specifieke kenmerken van de entiteit aan te scherpen of te wijzigen. De aldus geselecteerde beheersingsmaatregelen kunnen door de onafhankelijke IT-auditor worden getoetst om voldoende en relevante assurance-informatie te verkrijgen om tot een objectief oordeel te komen.

Gezien het feit dat de AVG organisaties verplicht om de bescherming van persoonsgegevens *aantoonbaar* te beheersen, ligt het voor de hand dat het PCF met name in attest-opdrachten zal worden gebruikt.

6. PCF en andere privacy-instrumenten van NOREA

Het PCF maakt deel uit van (en is gerelateerd aan) een breder privacy-instrumentarium dat NOREA beroepsbeoefenaren aanbiedt. Hiertoe behoren:

- *Handreiking Privacy Impact Assessments*
  Deze handreiking voor het uitvoeren van privacy impact assessments (PIA of DPIA, AVG: 'gegevensbeschermingseffectbeoordelingen') wordt op het moment van samenstelling van PCF 2.0 aan een revisie onderworpen om geheel in lijn te worden gebracht met de AVG. De huidige versie 1.2 uit 2015 zal naar verwachting in het tweede halfjaar van 2019 worden vervangen door een geactualiseerde versie. Het uitvoeren van DPIA's (zie het topic 'PIA' in dit document) geeft duidelijkheid in privacyrisico's. Voor de mitigatie daarvan kunnen de beheersingsdoelstellingen en -maatregelen uit het PCF als basis dienen.

- *Privacyprincipes en criteria ten behoeve van SOC 2*
  Aan de bestaande NOREA handreiking 'Guidance to Richtlijn (ISAE) 3000 Service Organization Control Reports for IT Service Organizations, based on the AICPA SOC 2 report model and the Trust Services Principles and Criteria' wordt momenteel een toevoeging gedaan. Hierin wordt beschreven hoe de privacycategorie opgenomen kan worden in een ISAE 3000/System and Organization Controls rapport gebaseerd op het SOC 2 report model en de onderliggende Trust Services Criteria. Hiertoe is een mapping gemaakt tussen de criteria uit SOC 2 Trust Services Criteria (ten aanzien van privacy) en de beheersdoelstellingen uit het PCF.

  In het SOC 2 rapport moeten de beheersingsdoelstellingen (criteria) uit SOC 2 worden gehanteerd. De toevoeging aan de handreiking beschrijft hoe de beheersingsmaatregelen uit het PCF als leidraad kunnen worden gebruikt voor het invullen van de SOC 2 privacycriteria, rekening houdend met het doel (objective) van de (service)organisatie en de 'points of focus'. Zodra de toevoeging gereed is zal die worden gepubliceerd op de website van de NOREA.

- *Keurmerk Privacy Audit Proof*
  Op basis van een assurance opdracht die heeft geresulteerd in een goedkeurend oordeel van een privacy (IT-) auditor kan aan een verwerkingsverantwoordelijke of verwerkende entiteit toestemming worden verleend het keurmerk (logo) 'Privacy-Audit-Proof' te gebruiken. Het PCF als onderliggend toetsingskader is hierbij uitgangspunt; gebruik van de beheersingsdoelstellingen van het PCF is verplicht, de beheersingsmaatregelen van het PCF gelden als illustratief. Het keurmerk kan slechts worden verleend op basis van een assurance-opdracht met een redelijke mate van zekerheid en zonder beperkingen in het oordeel, uitgevoerd op

basis van Richtlijn 3000 (Assurance -opdrachten door IT-auditors) en met hantering van het PCF als onderliggend toetsingskader. Het huidige Privacy Audit Proof-reglement wordt momenteel herzien en in lijn gebracht met deze uitgangspunten.

7. PCF en certificering volgens de AVG

De AVG zelf onderstreept het belang van certificeringsmechanismen om compliance met de AVG aan te tonen. Hoewel het PCF op dit moment formeel niet mag worden gezien als een verzameling criteria die een certificering zoals bedoeld in artikelen 42 en 43 van de AVG mogelijk maakt, voldoet het in beginsel wel aan de richtlijnen die de EDPB tot op heden over AVG-certificering heeft uitgebracht[5].

In Nederland heeft de Autoriteit Persoonsgegevens (AP) ervoor gekozen om de ontwikkeling van certificeringsschema's en criteria aan de markt over te laten. Auditorganisaties die 'AVG-certificaten' willen gaan afgeven, in feite de toekomstige Certificerende Instellingen (CI's), zullen daartoe eerst geaccrediteerd moeten worden. De AP heeft deze taak in handen gelegd van de Raad voor Accreditatie (RvA). Vooralsnog, naar de stand van augustus 2019, is er in Nederland nog geen enkele CI geaccrediteerd.

Bij de totstandkoming van het PCF is vanuit NOREA op verschillende momenten overleg gevoerd met de AP. De conceptversie van het PCF is ook aan de AP overlegd voor commentaar. In reactie daarop heeft de AP haar waardering uitgesproken voor (door)ontwikkeling van het PCF als een belangrijke standaard voor audit professionals.

Het is op dit moment nog niet mogelijk om een formeel privacy certificaat te verkrijgen zoals bedoeld in de artikelen 42 en 43 van de AVG. Wel is het mogelijk om op basis van het onderzoek van een onafhankelijke IT-auditor (RE) dat is uitgevoerd aan de hand van de criteria van het PCF, een privacy assurance verklaring te verkrijgen. Naar verwachting zullen deze twee stelsels (certificatie en assurance) in de toekomst meer naar elkaar toegroeien. Zodra zich op dit gebied nieuwe ontwikkelingen voordoen, zal dat op de website van de NOREA worden gemeld.

Organisaties die nu al geïnteresseerd zijn in het verkrijgen van een AVG-certificaat of privacy assurance verklaring wordt geadviseerd om contact op te nemen met een door het NOREA erkende IT-auditor (RE).

8. PCF en ISO 27001/ISO 27002

Persoonsgegevens moeten worden gezien als een bijzondere vorm van informatie, die in het kader van privacy adequaat beschermd dient te worden. Daarmee is er uiteraard een sterke relatie én een

[5] Met name "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Art. 42 & 43 of the Regulation" en "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)".

zekere overlap tussen het PCF en normenkaders die zich richten op informatiebeveiliging in zijn algemeenheid. Een voorbeeld van dit laatste zijn NEN-ISO/IEC ISO 27001 en 27002, die dienen als een certificatiestandaard voor een Informatiebeveiligingsmanagementsysteem (ISO 27001) en als een verzameling richtlijnen en best practices op het gebied van informatiebeveiliging (ISO 27002). Vele andere raamwerken (zoals bijvoorbeeld de Baseline Informatiebeveiliging Rijksdienst (BIR)), hebben hun wortels in ISO 27001/27002. In augustus 2019 heeft ISO de standaard ISO 27701 gepubliceerd, die een privacy-uitbreiding vormt op ISO 27001 en ISO 27002. In bijlage 3 van dit document wordt ingegaan op een aantal aspecten van de relatie tussen het PCF en ISO standaarden op het gebied van informatiebeveiliging en privacy.

9. Totstandkoming van het Privacy Control Framework

Het PCF is tussen november 2017 en april 2018 opgesteld door een werkgroep van NOREA. De eerste initiatieven van de werkgroep zijn verder uitgewerkt en gestructureerd tot versie 1.0 van dit document, dat door vakgenoten is getoetst en vervolgens is goedgekeurd door de Vaktechnische Commissie van NOREA. Versie 1.0 werd uitgebracht in mei 2018.

In de mei/juni 2019 is een update van het PCF (versie 2.0) gemaakt, dat vervolgens is getoetst door een klankbordgroep van leden van de Kennisgroep Privacy van NOREA, is beoordeeld en goedgekeurd door de Vaktechnische Commissie en in augustus 2019 is gepubliceerd. Voor deze Nederlandstalige versie is gebruik gemaakt van de Nederlandse vertaling van versie 1.0 van het PCF door SafeHarbour.

10. Wijzigingen in versie 2.0

In de update van versie 1.0 naar versie 2.0 van het PCF zijn de volgende wijzigingen doorgevoerd:

- tekstuele correctie en tekstuele aanscherpingen van alle delen;
- opmaakcorrectie (o.a. lemma's);
- aanvullingen in deel 1 (paragrafen 6, 7, 8);
- rationalisatie van bijlage 1 (relatie PCF-AVG);
- toevoeging van bijlage 3 (relatie PCF-ISO en cross reference);
- onderscheid in beheersmaatregelen voor verwerkingsverantwoordelijken en verwerkers (deel 3);
- Nederlandstalige versie van het PCF.

PCF 2.0 omvat 9 beheersingsmaatregelen minder dan PCF 1.0. Deze zijn samengevoegd of geïntegreerd met andere beheersingsmaatregelen en er is derhalve sprake van een herschikking, niet van een inhoudelijke wijziging. De 'vervallen' maatregelen zijn als zodanig aangeduid in deel 3.

11. Disclaimer

Het PCF is ontwikkeld om IT-auditors, (andere) professionals en entiteiten te ondersteunen bij de beoordeling van het stelsel van maatregelen voor een privacybeheersing. De resultaten, scores of aanbevelingen die voortkomen uit de toepassing van het PCF dienen niet zonder aanvullende informatie te worden gebruikt om te bepalen in hoeverre een entiteit aan de vereisten van de AVG voldoet of op welke wijze de AVG op een entiteit van toepassing is. Het PCF biedt geen juridisch advies, certificering of garanties met betrekking tot AVG-compliance. De praktische toepassing van de AVG wordt beschreven in uitvoeringsvoorschriften en richtlijnen. Het ligt in de verwachting dat deze -mede aan de hand van opgedane ervaringen- nog verder zullen worden uitgewerkt. We adviseren entiteiten die gebruikmaken van het PCF om ook samen met een juridisch gekwalificeerde professional de vereisten van de AVG te blijven monitoren, na te gaan hoe de AVG op hen van toepassing is en te bepalen hoe aan de vereisten kan worden voldaan.

Deel 2. Privacy Control Framework – Overzicht

De onderstaande tabel geeft een overzicht van het Privacy Control Framework. Het raamwerk bevat in totaal 95 beheersingsmaatregelen, verdeeld over 32 onderwerpen in 9 fasen van levenscyclusmanagement. In deel 3 worden de beheersingsmaatregelen per onderwerp/beheersingsdoelstelling weergegeven.

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
Management	PPO	Privacybeleid	De entiteit stelt een privacybeleid vast en communiceert dit. Dit beleid bevat de doelstellingen en verantwoordelijkheden met betrekking tot privacy en is in overstemming met geaccepteerde privacyprincipes en de van toepassing zijnde wet- en regelgeving.	5
	RRE	Afbakening van rollen en verantwoordelijkheden	De entiteit definieert duidelijke rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacydoelstellingen, en implementeert deze.	4
	PDI	Identificatie en classificatie van persoonsgegevens	De entiteit heeft een duidelijk beeld van en documenteert welke persoonsgegevens worden opgeslagen en verwerkt. Persoonsgegevens worden geïdentificeerd en er wordt op de juiste wijze mee omgegaan. In de maatregelen voor bescherming van persoonsgegevens wordt rekening gehouden met verschillen in de gevoeligheid van persoonsgegevens. Dit leidt tot identificatie van risico's en compliance met wet- en regelgeving.	4
	RMA	Risicomanagement	De entiteit identificeert, beoordeelt en beperkt systematisch en periodiek de factoren die het behalen van de privacydoelstellingen in gevaar kunnen brengen.	4

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
	PIA	Data protection impact assessments	De privacy-gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt.	5
	PIB	Beheer van privacyincidenten en inbreuken	De entiteit detecteert incidenten met betrekking tot privacy en handelt deze af. Op privacy-gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken en er worden maatregelen genomen om toekomstige inbreuken te voorkomen.	8
	SCO	Competenties medewerkers	Medewerkers die vanuit hun functie toegang hebben tot persoonsgegevens of processen beheren waarin persoonsgegevens worden verwerkt, beschikken over de benodigde competenties met betrekking tot privacy om hun taken naar behoren te kunnen vervullen.	4
	SAT	Bewustwording en training medewerkers	De medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacybeleid en de richtlijnen binnen de organisatie, en hun verantwoordelijkheden met betrekking tot privacy. De entiteit implementeert programma's om bewustwording te bereiken en op peil te houden..	3
	LRC	Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten	De entiteit houdt voldoende rekening met privacyrisico's die voortkomen uit veranderingen binnen de entiteit (structuur en strategie) en wet- en regelgeving.	1
Informeren	PST	Privacyverklaring	De entiteit informeert betrokkenen op transparante wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens.	2

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
Keuze en toestemming	CFR	Toestemmingsraamwerk	De entiteit verkrijgt indien vereist of noodzakelijk toestemming van de betrokkene om persoonsgegevens te verwerken.	4
Verzamelen	DMI	Minimale gegevensverwerking	De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt.	2
Gebruiken, opslaan en verwijderen	ULI	Doelbinding	Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij: de betrokkene toestemming verleent; of dit wettelijk vereist is.	2
	PBD	Privacyarchitectuur (Gegevens-bescherming door ontwerp en door standaard-instellingen)	De entiteit neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het privacybeleid, de privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht.	3
	DRE	Bewaren van gegevens	Persoonsgegevens worden niet langer bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld.	2
	DDA	Verwijdering, vernietiging en anonimiseren	Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken.	2

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
	URE	Gebruik en beperking	Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen of wanneer er sprake is van specifieke juridische restricties door lokale autoriteiten. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld.	2
Inzage en kwaliteit van gegevens	DAR	Verzoek tot inzage	Een inzageverzoek van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen nagaan welke persoonsgegevens van hen worden verwerkt en op welke manier.	3
	DCR	Verzoek tot rectificatie	Een rectificatieverzoek van de betrokkene wordt op de juiste wijze afgehandeld. Betrokkenen kunnen bepalen of hun persoonsgegevens juist/up-to-date en zo nodig geactualiseerd zijn en zij kunnen deze (laten) corrigeren.	3
	DDR	Verzoek tot wissen	Een verzoek tot het wissen van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen bepalen welke persoonsgegevens zij willen laten wissen, mits aan de geldende criteria wordt voldaan.	3
	DPR	Verzoek tot overdracht	Een verzoek tot overdracht van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen hun persoonsgegevens laten overdragen aan een andere entiteit, mits aan de geldende criteria wordt voldaan.	3
	ACD	Juistheid en volledigheid van gegevens	Vastgelegde procedures voor het valideren, aanpassen en bijwerken van persoonsgegevens waarborgen de juistheid en volledigheid van persoonsgegevens	2

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
Verstrekken	TPD	Verstrekking aan derden en registratie	Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis of voor andere doeleinden dan waarover de betrokkene is geïnformeerd.	1
	TPA	Overeenkomsten met derden	Bij de verwerving van oplossingen en diensten (gerelateerd aan persoonsgegevens) van derden wordt voldoende aandacht besteed aan privacyoverwegingen en -vereisten, waardoor geborgd wordt op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd.	3
	DTR	Doorgifte van persoonsgegevens	Persoonsgegevens worden niet doorgegeven (d.w.z. verplaatst, weergegeven of geprint op een andere locatie) aan landen die geen toereikend rechtskader ten aanzien van privacy hebben.	2
Gegevens-beveiliging	ISP	Programma informatiebeveiliging	Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde verstrekking of verlies.	7
	IAM	Identiteit en toegangsbeheer	Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans opop ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers.	1
	STR	Veilige gegevensoverdracht	Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen.	1
	ENC	Versleuteling en eindpuntbeveiliging	Inbreuk in verband met persoonsgegevens/ datalek (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) wordt voorkomen door middel van versleuteling.	4

Fase levenscyclus	Code	Onderwerp	Beheersingsdoelstelling	# Beheersings-maatregel
	LOG	Registreren van toegang	Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen.	1
Monitoren en handhaven	REV	Beoordeling van compliance met privacywetgeving	Adequaat toezicht op de interne organisatie en derden waarborgt dat de entiteit voldoet aan de wet- en regelgeving met betrekking tot privacy en vermindert het risico op inbreuk in verband met persoonsgegevens of verlies hiervan.	1
	MON	Periodiek monitoren van privacybeheersings-maatregelen	Systematische en periodieke evaluatie van privacyprocessen en beheersingsmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving.	3

Deel 3. Privacy Control Framework – Beheersingsmaatregelen

De volgende pagina's geven een opsomming van de beheersingsmaatregelen van het PCF, geordend per onderwerp en per fase uit het levenscyclusmodel. Voor elk onderwerp wordt de beheersings-doelstelling genoemd, evenals de gerelateerde kernelementen uit de AVG.

Voor elke beheersingsmaatregel is in een afzonderlijke kolom aangegeven of die maatregel van toepassing is voor een verwerkingsverantwoordelijke ('VV'), verwerker ('V'), of beide ('VV, V').

Management

Privacybeleid (PPO)		
Beheersingsdoelstelling: De entiteit stelt een privacybeleid vast en communiceert dit. Dit beleid bevat de doelstellingen en verantwoordelijkheden met betrekking tot privacy en is in overstemming met geaccepteerde privacyprincipes en de van toepassing zijnde wet- en regelgeving.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
PPO01	De entiteit heeft een gedocumenteerd privacybeleid vastgesteld en heeft dit gecommuniceerd aan de interne medewerkers en externe belanghebbenden. Het privacybeleid wordt jaarlijks door het management geëvalueerd en goedgekeurd.	VV, V
PPO02	Het management brengt zijn commitment (en verantwoordelijkheid voor) solide en rechtmatige privacyprincipes tot uitdrukking.	VV, V
PPO03	Het privacybeleid bevat de doelstellingen van de entiteit met betrekking tot privacy en de bescherming van persoonsgegevens (zie ook DMI02 en ULI02),	VV, V
PPO04	(a) De entiteit neemt bij elke verwerking van persoonsgegevens de algemeen geaccepteerde en wettelijke privacyprincipes in acht en legt vast op welke wijze hieraan wordt voldaan. (b) De entiteit zorgt ervoor dat voor elke verwerking van persoonsgegevens gedocumenteerde instructies van contractuele partners vastgelegd zijn.	VV V
PPO05	De entiteit heeft criteria opgesteld en vastgelegd om aan te tonen dat elke verwerking van persoonsgegevens rechtmatig is.	VV, V
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Rechtmatigheid van de verwerking • Register van de verwerkingsactiviteiten		

Afbakening van rollen en verantwoordelijkheden (RRE)		
Beheersingsdoelstelling: De entiteit definieert duidelijke rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacydoelstellingen, en implementeert deze.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
RRE01	De entiteit stelt bij elke verwerking van persoonsgegevens vast en documenteert of zij verwerker of verwerkingsverantwoordelijke is.	V, VV
~~RRE02~~	*Vervangen door RRE03(b).*	
RRE03	(a) In de gevallen dat de entiteit als verwerkingsverantwoordelijke optreedt, sluit deze een overeenkomst met de verwerkers waarin de verantwoordelijkheden van de verwerker met betrekking tot privacy zijn vastgelegd. Indien de entiteit als gezamenlijke verwerkingsverantwoordelijke optreedt, worden afspraken gemaakt met de andere verwerkingsverantwoordelijke. (b) In de gevallen dat een entiteit optreedt als verwerker, is er een overeenkomst met de verwerkingsverantwoordelijke(n) waarin de verantwoordelijkheden van de verwerker met betrekking tot privacy zijn vastgelegd. Als verwerking verder wordt uitbesteed aan een subverwerker, is er een overeenkomst met de subverwerker waarin de verantwoordelijkheden van de subverwerker met betrekking tot privacy zijn vastgelegd.	VV V
RRE04	De entiteit belast een aangewezen persoon, zoals een privacy officer of functionaris voor gegevensbescherming (FG), met het coördineren van en toezicht houden op privacybescherming. De taken bevoegdheden en verantwoordelijkheden van deze persoon worden duidelijk omschreven en regelmatig herzien.	VV, V
RRE05	De taken en verantwoordelijkheden van individuele medewerkers voor wat betreft de bescherming van persoonsgegevens en naleving van de privacyprincipes worden vastgesteld en gecommuniceerd.	VV, V
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker • Register van de verwerkingsactiviteiten • Functionaris voor gegevensbescherming • Doorgiften van persoonsgegevens aan derde landen of internationale organisaties		

Identificatie en classificatie van persoonsgegevens (PDI)		
Beheersingsdoelstelling: De entiteit heeft een duidelijk beeld van en documenteert welke persoonsgegevens worden opgeslagen en verwerkt. Persoonsgegevens worden geïdentificeerd en er wordt op de juiste wijze mee omgegaan. In de maatregelen voor bescherming van persoonsgegevens wordt rekening gehouden met verschillen in de gevoeligheid van persoonsgegevens. Dit leidt tot identificatie van risico's en compliance met wet- en regelgeving.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
PDI01	De entiteit identificeert en documenteert verwerking van persoonsgegevens aan de hand van een gedocumenteerd proces, en classificeert deze gegevens als zodanig. Dit omvat tevens processen, systemen en derden die persoonsgegevens verwerken.	VV, V
PDI02	De entiteit maakt duidelijk onderscheid tussen de verwerking van (a) persoonsgegevens en (b) bijzondere categorieën van persoonsgegevens.	VV, V
PDI03	De entiteit heeft een procedure opgesteld om te bepalen of bij bestaande of geplande verwerking van persoonsgegevens bijzondere categorieën van persoonsgegevens worden verwerkt. Als dit het geval is, wordt de rechtmatigheid van de (geplande) verwerking uitvoerig beoordeeld en gedocumenteerd en worden maatregelen getroffen om veilige verwerking volgens de geldende voorschriften te waarborgen.	VV
PDI04	(a) De entiteit houdt een register bij van de verwerkingsactiviteiten met daarin de kenmerken van deze activiteiten (rechtsgrond, doel, categorieën van gegevens en betrokkenen, ontvangers, beveiligingsmaatregelen). (b) De entiteit houdt een register bij van de verwerkingsactiviteiten die voor elke ververkingsverantwoordelijke worden uitgevoerd met daarin de kenmerken van deze activiteiten (contactgegevens van verwerkingsverantwoordelijken, doorgiften, beveiligingsmaatregelen).	VV V
Gerelateerde kernelementen van de AVG: • Register van de verwerkingsactiviteiten • Privacyprincipes • Beveiliging van de verwerking		

Risicomanagement (RMA) *Beheersingsdoelstelling:* De entiteit identificeert, beoordeelt en beperkt systematisch en periodiek de factoren die het behalen van de privacydoelstellingen in gevaar kunnen brengen.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
RMA01	Er is een proces ingericht om: a. periodiek gebeurtenissen en factoren te identificeren die het behalen van de privacydoelstellingen in gevaar brengen; b. de gevolgen van deze gebeurtenissen en factoren en de kans dat zij plaatsvinden te beoordelen, om vervolgens een passende risicorespons en beheersingsmaatregelen te formuleren.	VV, V
~~RMA02~~	*Samengevoegd met RMA01.*	
RMA03	Wanneer nieuwe of gewijzigde privacyrisico's worden gesignaleerd, worden de privacyrisicobeoordeling en de risicobeheerstrategieën herzien en zo nodig bijgewerkt.	VV, V
RMA04	Acceptatiecriteria voor privacyrisico's worden vastgesteld, goedgekeurd, gedocumenteerd en toegepast.	VV, V
RMA05	De entiteit brengt de beheersingsmaatregelen in kaart die nodig zijn om privacyrisico's te mitigeren en implementeert deze. De voortgang van de implementatie wordt gevolgd en beoordeeld.	VV, V
Gerelateerde kernelementen van de AVG: • Gegevensbeschermingseffectbeoordeling • Gegevensbescherming door ontwerp / door standaardinstellingen		

Data protection impact assessments (PIA) *Beheersingsdoelstelling:* De privacy-gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		*Bevindingen/ toetsing:*
PIA01	De entiteit beoordeelt aan de hand van een gedocumenteerd proces de effecten op privacybescherming van nieuwe of sterk gewijzigde processen, producten en diensten (DPIA).	VV
PIA02	Bij de DPIA wordt vastgesteld: a. de aard van de geplande verwerkingen; b. hun doelstelling, noodzaak, en proportionaliteit; c. de privacyrisico's die beoogde verwerkingen met zich meebrengen voor betrokkenen; d. welke maatregelen moeten worden genomen om deze risico's te beperken.	VV
~~PIA03~~	*Samengevoegd met PIA02*.	
PIA04	Alle relevante belanghebbenden zijn bij de DPIA betrokken en de specifieke richtlijnen van de toezichthoudende autoriteit ten aanzien van beoordelingscriteria worden nageleefd.	VV
PIA05	De entiteit documenteert welke systemen en software persoonsgegevens verwerken en houdt bij welke wijzigingen hierin zijn doorgevoerd.	VV
PIA06	Een verandermanagementproces is vastgesteld om ervoor zorg te dragen dat de in de DPIA goedgekeurde privacymaatregelen zijn geïmplementeerd voordat de wijziging wordt doorgevoerd.	VV
Gerelateerde kernelementen van de AVG: • Gegevensbeschermingseffectbeoordeling		

Beheer van privacyincidenten en inbreuken (PIB) *Beheersingsdoelstelling:* De entiteit detecteert incidenten met betrekking tot privacy en handelt deze af. Op privacy-gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken en er worden maatregelen genomen om toekomstige inbreuken te voorkomen.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
PIB01	De entiteit heeft een formeel, omvattend proces vastgesteld gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens, waarin het volgende is vastgelegd: a. De verantwoordelijkheid van medewerkers om de aangewezen privacyofficer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens; b. De privacyfunctionaris of FG (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft. Indien er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacyfunctionaris de aard van de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevensregisters en betrokkenen in kwestie. c. De privacyfunctionaris of FG initieert en coördineert de nodige maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd (zoals de verwerkingsverantwoordelijke wanneer de entiteit de rol van verwerker heeft of de toezichthouder als de entiteit verwerkingsverantwoordelijke is). d. De privacyfunctionaris of FG houdt toezicht op de voortgang van de corrigerende maatregelen en licht het management in (en, indien van toepassing, de verwerkingsverantwoordelijke en de teozichthouder).	VV, V
~~PIB02~~	*Samengevoegd met PIB06.*	
PIB03	Het proces bevat een duidelijke escalatieprocedure, gebaseerd op het type en/of de ernst van het incident, tot aan het inwinnen van juridisch advies en het inlichten van het hoogste management. In de procedure staan de criteria voor het opnemen van contact met rechtshandhavende-, toezichthoudende of andere autoriteiten.	VV, V
PIB04	(a) De entiteit heeft een beleid ten aanzien van het melden van inbreuk op de beveiliging. Dit zorgt ervoor dat de toezichthoudende autoriteit tijdig wordt	VV

	ingelicht wanneer het waarschijnlijk is dat een inbreuk risico's voor de rechten en vrijheden van de natuurlijke persoon met zich meebrengt. (b) De entiteit heeft een beleid ten aanzien van het melden van een inbreuk op de beveiliging. Dit zorgt ervoor dat de betreffende verwerkingsverantwoordelijke tijdig wordt ingelicht over een dergelijke (mogelijke) inbreuk.	V
PIB05	(a) In het geval van een inbreuk wordt alle vereiste informatie met betrekking tot de inbreuk verzameld en gemeld aan de toezichthoudende autoriteit. Tot deze informatie behoren ook de oorzaak en mitigerende maatregelen. (b) In het geval van een (mogelijke) inbreuk wordt alle vereiste informatie met betrekking tot de inbreuk verzameld en gemeld aan de verwerkingsverantwoordelijke voor de betreffende verwerking. Tot deze informatie behoren ook de oorzaak en mitigerende maatregelen.	VV V
PIB06	De aangewezen privacy officer of FG is belast met de algehele verantwoordelijkheid voor de melding van de inbreuk. De privacy officer documenteert alle gemaakte overwegingen bij het bepalen van de meldplicht.	VV, V
PIB07	In de procedure voor beheer van privacyincidenten en -inbreuken staat dat, op basis van de evaluatie van incidenten/inbreuken, correcties en verbeteringen worden doorgevoerd, en dat de informatie wordt gebruikt in bewustwordingsprogramma's voor medewerkers.	VV, V
PIB08	In de procedure voor beheer van privacyincidenten en -inbreuken is het volgende vastgelegd: a. na elk beveiligingsincident en inbreuk met betrekking tot persoonsgegevens ('datalekken') en elke grootschalige inbreuk in verband met persoonsgegevens wordt een formele incidentbeoordeling uitgevoerd, waarbij indien nodig externe expertise wordt ingeschakeld; b. incidenten worden periodiek geëvalueerd en de noodzakelijke verbeteringen worden geïdentificeerd op basis van: • de onderliggende oorzaak van het incident; • incidentpatronen; • wijzigingen in de interne controle en wetgeving; c. De resultaten van de periodieke evaluatie en voortgang van de verbeteringen worden gerapporteerd aan en beoordeeld door het management.	VV, V
PIB09	De procedure voor beheer van inbreuken wordt ten minste eenmaal per jaar herzien en tevens kort na de implementatie van ingrijpende wijzigingen in systemen of procedures.	VV, V
Gerelateerde kernelementen van de AVG: • Inbreuk in verband met persoonsgegevens		

Competenties medewerkers (SCO)		
Beheersingsdoelstelling: Medewerkers die vanuit hun functie toegang hebben tot persoonsgegevens of processen beheren waarin persoonsgegevens worden verwerkt, beschikken over de benodigde competenties met betrekking tot privacy om hun taken naar behoren te kunnen vervullen.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
SCO01	De entiteit legt vast over welke competenties met betrekking tot privacy medewerkers die met persoonsgegevens werken moeten beschikken. De entiteit stelt legt daarnaast vast hoe deze competenties kunnen worden verworven (o.a. door trainingen).	VV, V
SCO02	De entiteit documenteert in hoeverre individuele medewerkers over deze competenties beschikken en heeft een procedure opgesteld om een gebrek aan vaardigheden aan te vullen.	VV, V
SCO03	De entiteit besteedt bij de werving en onboarding van nieuwe medewerkers die belast zijn met beveiliging van persoonsgegevens en compliance met privacyprincipes aandacht aan competenties met betrekking tot privacy. De omgang met privacy is een van de punten in individuele beoordelingsgesprekken.	VV, V
SCO04	Het management evalueert jaarlijks de toewijzing van personeel, budgetten en andere middelen aan het privacyprogramma.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Privacyprincipes • Functionaris voor gegevensbescherming		

Bewustwording en training medewerkers (SAT)		
Beheersingsdoelstelling: De medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacybeleid en de richtlijnen binnen de organisatie, en hun verantwoordelijkheden met betrekking tot privacy De entiteit implementeert programma's om bewustwording te bereiken en op peil te houden..		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		*Bevindingen/ toetsing:*
SAT01	Ten minste eenmaal per jaar wordt voor alle medewerkers een bewustwordingscursus ten aanzien van privacy en beveiliging georganiseerd. Nieuwe medewerkers, contractanten en anderen wordt verplicht om binnen een maand na aanvang van de overeenkomst een vergelijkbare training te volgen, zodat zij op de hoogte zijn van het privacybeleid van de entiteit en de implicaties hiervan.	VV, V
SAT02	Verdiepende (interne of externe) privacytraining wordt aangeboden op basis van de benodigde privacycompetenties van medewerkers (zie SCO). Tijdens de training worden het beleid en de procedures met betrekking tot privacy en relevant beveiligingsbeleid en -procedures behandeld, alsook overwegingen van wettelijke of regelgevende aard, de incidentrespons en gerelateerde onderwerpen. Een dergelijke training is: • jaarlijks verplicht voor alle medewerkers die toegang hebben tot persoonsgegevens of belast zijn met de bescherming ervan; • afgestemd op de verantwoordelijkheden van de medewerker binnen zijn of haar functie en de benodigde competenties.	VV, V
SAT03	Trainingen en bewustwordingscursussen worden geëvalueerd en geactualiseerd om aan te sluiten bij de huidige wet- en regelgeving, sectorspecifieke eisen en het beleid en de procedures van de entiteit.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Privacyprincipes		

Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC) *Beheersingsdoelstelling:* De entiteit houdt voldoende rekening met privacyrisico's die voortkomen uit veranderingen binnen de entiteit (structuur en strategie) en wet- en regelgeving.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		
LRC01	De entiteit richt een proces in om het effect op de privacyvereisten te monitoren, beoordelen en te behandelen van wijzigingen in: a. wet- en regelgeving; b. sectorspecifieke eisen, best practices en richtlijnen; c. overeenkomsten, waaronder Service Level Agreements met derden (wijzigingen van de bepalingen inzake privacy en beveiliging in overeenkomsten worden op adequate wijze geëvalueerd en goedgekeurd voordat zij worden uitgevoerd); d. bedrijfsactiviteiten en processen; e. personen die worden belast met de verantwoordelijkheid voor privacy en beveiliging; f. technologie (voordat deze wordt geïmplementeerd).	VV, V
Gerelateerde kernelementen van de AVG: • Gegevensbeschermingseffectbeoordeling • Rechtmatigheid van de verwerking		

Informeren

Privacyverklaring (PST) *Beheersingsdoelstelling:* De entiteit informeert betrokkenen op transparante wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens.		
Fase informatielevenscyclusmanagement: **Informeren**		
Beheersingsmaatregelen:		
PST01	In de privacyverklaring van de entiteit staat: a. welke persoonsgegevens worden verzameld, waar deze informatie vandaan komt, de doeleinden voor de verzameling en de betreffende rechtsgronden voor de verwerking; b. wat de gevolgen zijn, voor zover daar sprake van is, als de betrokkene de gevraagde gegevens niet verstrekt; c. informatie over verdere verwerking (indien van toepassing); d. informatie over de rechten van betrokkenen en de wijze waarop zij die rechten kunnen uitoefenen (zie ook URE, DAR, DCR, DDR, DPR).	VV
PST02	De privacyverklaring: a. is gemakkelijk toegankelijk en beschikbaar voor betrokkenen op het moment dat voor het eerst persoonsgegevens van de betrokkene worden verzameld; b. wordt tijdig beschikbaar gesteld (ten tijde van of voorafgaand aan het moment dat persoonsgegevens worden verzameld, of zo spoedig mogelijk erna) zodat de betrokkene de keuze heeft om de persoonsgegevens wel of niet te verstrekken; c. is duidelijk van een datum voorzien, zodat betrokkenen kunnen zien of de verklaring is aangepast sinds zij deze hebben gelezen of sinds de laatste keer dat zij persoonsgegevens aan de entiteit hebben verstrekt; d. is eenvoudig te begrijpen en leesbaar.	VV
Gerelateerde kernelementen van de AVG: • Rechten van de betrokkene • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker • Privacyprincipes		

Keuze en toestemming

Toestemmingsraamwerk (CFR) *Beheersingsdoelstelling:* De entiteit verkrijgt indien vereist of noodzakelijk toestemming van de betrokkene om persoonsgegevens te verwerken.		
Fase informatielevenscyclusmanagement: **Keuze en toestemming**		
Beheersingsmaatregelen:		*Bevindingen/ toetsing:*
CFR01	In de privacyverklaring beschrijft de entiteit op duidelijke en beknopte wijze: a. welke keuzes de betrokkene heeft met betrekking tot de verzameling, het gebruik, en de verstrekking van persoonsgegevens; b. wat de betrokkene moet doen om deze keuzes te maken (zoals het aanvinken van een vakje om aan te geven dat hij/zij geen marketingmateriaal wenst te ontvangen); c. de mogelijkheid om de contactvoorkeuren aan te passen en hoe de betrokkene dit doet; d. wat de gevolgen zijn als de persoonsgegevens die nodig zijn voor een transactie of dienst niet worden verstrekt; e. wat de gevolgen zijn als de persoon weigert persoonsgegevens te verstrekken (transacties kunnen bijvoorbeeld mogelijk niet worden verwerkt); f. wat de gevolgen zijn van het niet verlenen of intrekken van toestemming (als de persoon bijvoorbeeld geen informatie wenst te ontvangen over producten en diensten, wordt hij of zij mogelijk niet op de hoogte gebracht van acties).	VV
CFR02	Wanneer de verwerking is gebaseerd op de grondslag toestemming: a. verkrijgt en documenteert de entiteit tijdig de toestemming van de betrokkene (ten tijde van of voorafgaand aan het moment dat de persoonsgegevens worden verzameld, of kort erna); b. legt de entiteit de voorkeuren van de betrokkene vast (schriftelijk of elektronisch);	VV

	c. documenteert de entiteit wijzigingen in de contactvoorkeuren en verwerkt deze; d. zorgt de entiteit dat de voorkeuren van de betrokkene tijdig worden verwerkt; e. bewaart de entiteit de informatie om aan kunnen te tonen dat de betrokkene toestemming heeft verleend.	
CFR03	De entiteit verzamelt of verwerkt geen bijzondere categorieën van persoonsgegevens, tenzij de entiteit hiervoor een wettelijke grondslag heeft. Wanneer de uitdrukkelijke toestemming van de betrokkene de wettelijke grondslag is voor de verwerking van bijzondere categorieën van persoonsgegevens, heeft de betrokkene door middel van een duidelijke actieve handeling ingestemd met het gebruik of de verstrekking van bijzondere categorieën van persoonsgegevens. De entiteit verkrijgt de uitdrukkelijke toestemming rechtstreeks van de betrokkene en documenteert/bewaart het bewijs dat deze toestemming is verleend, bijvoorbeeld door de persoon te vragen een vakje aan te vinken of een formulier te ondertekenen.	VV
CFR04	Wanneer de verwerking van persoonsgegevens berust op toestemming, faciliteert de entiteit de uitoefening van het recht van de betrokkene om zijn toestemming te allen tijde in te trekken.	VV
Gerelateerde kernelementen van de AVG: • Rechtmatigheid van de verwerking • Voorwaarden voor toestemming • Rechten van de betrokkene		

Verzamelen

Minimale gegevensverwerking (DMI) *Beheersingsdoelstelling:* De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt.		
Fase informatielevenscyclusmanagement: **Verzamelen**		
Beheersingsmaatregelen:		
DMI01	De entiteit richt een proces en procedures in om: a. te bepalen welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking en welke persoonsgegevens optioneel zijn; b. de verwerking van persoonsgegevens te beperken tot het voor het doel noodzakelijke minimum; c. periodiek na te gaan of de verwerking van persoonsgegevens nog noodzakelijk is voor de producten en/of diensten van de entiteit.	VV
DMI02	In het privacybeleid van de entiteit is opgenomen dat minimale gegevensverwerking een privacyprincipe is (zie PPO).	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Gegevensbescherming door ontwerp / door standaardinstellingen		

Gebruiken, opslaan en verwijderen

Doelbinding (ULI) *Beheersingsdoelstelling:* Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij: • de betrokkene toestemming verleent; of • dit wettelijk vereist is.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
ULI01	De entiteit richt een proces en procedures in om: a. de verstrekking en het gebruik van persoonsgegevens te beperken tot de gerechtvaardigde doeleinden die worden genoemd in het privacybeleid en de privacyverklaring van de entiteit; b. bij voortduring te waarborgen dat de verstrekking en het gebruik van persoonsgegevens overeenkomstig de toestemming van de betrokkene en de betreffende wet- en regelgeving is.	VV
ULI02	In het privacybeleid van de entiteit is opgenomen dat doelbinding een privacyprincipe is (zie PPO).	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Gegevensbescherming door ontwerp / door standaardinstellingen		

Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) (PBD) *Beheersingsdoelstelling:* De entiteit neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het solide privacybeleid, de privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
PBD01	Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt de entiteit zo vroeg mogelijk in het ontwerpproces rekening met de privacyprincipes en privacyrisico's. Het risico op strijdigheid tussen het ontwerp en de rechten en vrijheden van betrokkenen (en het privacybeleid van de entiteit) is geïdentificeerd en aangepakt. Wanneer de entiteit diensten van derden bij deze activiteiten betrekt, verplicht de entiteit deze partijen om dezelfde risicomanagementactiviteiten ten aanzien van privacy te hanteren.	VV
PBD02	De beoordeling van privacyrisico's is een inherent en gedocumenteerd onderdeel van de projectmethodiek en/of het ontwikkelingsproces van de entiteit.	VV
PBD03	Wanneer systemen, diensten en producten waarbij persoonsgegevens worden verwerkt privacy-gerelateerde opties bieden, zijn deze standaard ingesteld op de meest beperkende optie met betrekking tot privacy.	VV
Gerelateerde kernelementen van de AVG: • Gegevensbescherming door ontwerp / door standaardinstellingen • Privacyprincipes		

Bewaren van gegevens (DRE) *Beheersingsdoelstelling:* Persoonsgegevens worden niet langer bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
DRE01	De entiteit: a. documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens; b. zorgt dat persoonsgegevens niet langer worden bewaard dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of wettelijke verplichting. c. documenteert voor elke verwerking van persoonsgegevens de betreffende bewaartermijn; d. informeert betrokkenen in de privacyverklaring over het beleid ten aanzien van bewaartermijnen; e. slaat gearchiveerde kopieën en back-ups op, bewaart en verwijdert deze overeenkomstig het bewaarbeleid; f. instrueert verwerkers over bewaartermijnen.	VV
DRE02	Bij het vaststellen van bewaarprocedures worden wettelijke en contractuele bewaartermijnen in acht genomen; deze wijken mogelijk af van de normale beleidsregels.	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker		

Verwijdering, vernietiging en anonimisatie (DDA) *Beheersingsdoelstelling:* Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
DDA01	De entiteit heeft een gedocumenteerde procedure ingericht om te waarborgen dat: a. het wissen en vernietigen van persoonsgegevens geschiedt conform het bewaarbeleid, ongeacht de vorm waarin deze zijn opgeslagen (zoals elektronisch, op optische media, of op papier); b. de verwijdering van originele, gearchiveerde gegevens, back-ups en persoonlijke kopieën conform het vernietigingsbeleid plaats-vindt; c. de verwijdering van persoonsgegevens op een adequate wijze wordt vastgelegd. De entiteit zorgt er daarnaast voor dat: d. persoonsgegevens worden gelokaliseerd en verwijderd of terug-gebracht, voor zover dit technisch mogelijk is. e. persoonsgegevens die niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of gegevens die op grond van wet- en regelgeving moeten worden verwijderd, op regelmatige en syste-matische basis worden vernietigd, gewist of geanonimiseerd.	VV
DDA02	Bij het vaststellen van procedures voor verwijdering, vernietiging en ver-mindering van persoonsgegevens worden contractbepalingen in acht ge-nomen indien deze afwijken van de normale beleidsregels.	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker • Beveiliging van de verwerking • Gegevensbescherming door ontwerp / door standaardinstellingen		

Gebruik en beperking (URE)		
Beheersingsdoelstelling: Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen of wanneer er sprake is van specifieke juridische restricties door lokale autoriteiten. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
~~URE01~~	*Samengevoegd met PST01.*	
URE02	De entiteit heeft een proces ingericht om adequaat te handelen wanneer betrokkenen hun recht op beperking van of bezwaar tegen de verwerking uitoefenen.	VV
URE03	De entiteit heeft vastgesteld of lidstaatrechtelijke bepalingen de verwerking van persoonsgegevens beperken (bijvoorbeeld ter bescherming van de nationale of openbare veiligheid) en kan aantonen dat deze beperkingen worden gehandhaafd.	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Rechtmatigheid van de verwerking • Rechten van de betrokkene • Doorgiften van persoonsgegevens aan derde landen of internationale organisaties		

Inzage en kwaliteit van gegevens

Verzoek tot inzage (DAR) *Beheersingsdoelstelling:* Een inzageverzoek van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen nagaan welke persoonsgegevens van hen worden verwerkt en op welke manier.		
Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**		
Beheersingsmaatregelen:		
DAR01	De entiteit heeft procedures ingericht om adequaat te reageren op inzageverzoeken van betrokkenen. Indien de betrokkene het recht op inzage uitoefent, verstrekt de entiteit aan de betrokkene informatie over de aard van de verwerkte persoonsgegevens en de kenmerken van de verwerking (bijv. het doel, de ontvangers, de bewaartermijnen, het bestaan van geautomatiseerde besluitvorming).	VV
~~DAR02~~	*Samengevoegd met PST01*.	
DAR03	De entiteit heeft een proces ingericht om tijdig een kopie van de verwerkte persoonsgegevens aan de betrokkene te verstrekken in een gangbare elektronische vorm.	VV
DAR04	De entiteit verifieert de identiteit van de betrokkene alvorens informatie te verstrekken.	VV
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Gegevensbescherming door ontwerp / door standaardinstellingen • Rechten van de betrokkene		

Verzoek tot rectificatie (DCR)		
Beheersingsdoelstelling: Een rectificatieverzoek van de betrokkene wordt op de juiste wijze afgehandeld. Betrokkenen kunnen bepalen of hun persoonsgegevens correct/up-to-date zijn en zij kunnen deze corrigeren.		
Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**		
Beheersingsmaatregelen:		
DCR01	De entiteit heeft procedures ingericht om adequaat te reageren op rectificatieverzoeken van betrokkenen. Indien de betrokkene het recht op rectificatie uitoefent, corrigeert de entiteit de persoonsgegevens onverwijld.	VV
~~DCR02~~	*Samengevoegd met PST01.*	
DCR03	De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen.	VV
DCR04	De entiteit stelt partijen waar de persoonsgegevens aan zijn verstrekt op de hoogte van de wijzigingen.	VV
Gerelateerde kernelementen van de AVG: • Rechten van de betrokkene		

Verzoek tot wissen (DDR) *Beheersingsdoelstelling:* Een verzoek tot het wissen van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen bepalen welke persoonsgegevens zij willen laten wissen, mits aan de geldende criteria wordt voldaan.		
Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**		
Beheersingsmaatregelen:		
DDR01	De entiteit heeft procedures ingericht om adequaat te reageren op een verzoek tot het wissen van persoonsgegevens ('recht op vergetelheid'). Indien de betrokkene het recht op gegevenswissing uitoefent, toetst de entiteit de gronden van het verzoek aan de geldende criteria (bijv. de verwerking berust op toestemming, de verwerking is onrechtmatig, het doel is niet langer geldig, wettelijke vereisten voor bewaren). Als de grond gerechtvaardigd is, wist de entiteit de persoonsgegevens onverwijld.	VV
DDR02	Indien van toepassing stelt de entiteit andere verwerkingsverantwoordelijken waar de persoonsgegevens aan zijn verstrekt op de hoogte van het verzoek van de betrokkene om persoonsgegevens te laten wissen. Indien de persoonsgegevens worden verwerkt door een verwerker, instrueert de entiteit de verwerker de gegevens te wissen.	VV
~~DDR03~~	*Samengevoegd met PST01.*	
DDR04	De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen.	VV
Gerelateerde kernelementen van de AVG: • Rechten van de betrokkene		

Verzoek tot overdracht (DPR) *Beheersingsdoelstelling:* Een verzoek tot overdracht van persoonsgegevens van de betrokkene wordt op de juiste wijze afgehandeld en betrokkenen kunnen hun persoonsgegevens laten overdragen aan een andere entiteit, mits aan de geldende criteria wordt voldaan.		
Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**		
Beheersingsmaatregelen:		
DPR01	De entiteit heeft procedures ingericht om adequaat te reageren op een verzoek tot overdracht van persoonsgegevens. Indien de betrokkene het recht op overdracht uitoefent, toetst de entiteit de gronden van het verzoek aan de geldende criteria (bijv. de verwerking berust op toestemming, de verwerking wordt via geautomatiseerde procedés verricht). Als de grond gerechtvaardigd is, draagt de entiteit de persoonsgegevens zonder onnodige vertraging over.	VV
DPR02	Als het technisch gezien mogelijk is, draagt de entiteit de persoonsgegevens rechtstreeks over aan de door de betrokkene aangewezen entiteit (verwerkingsverantwoordelijke).	VV
~~DPR03~~	*Samengevoegd met PST01.*	
DPR04	De entiteit verifieert de identiteit van de betrokkene alvorens het verzoek in te willigen.	VV
Gerelateerde kernelementen van de AVG: • Rechten van de betrokkene • Recht op overdraagbaarheid van gegevens		

Juistheid en volledigheid van gegevens (ACD) *Beheersingsdoelstelling:* Vastgelegde procedures voor het valideren, aanpassen en bijwerken van persoonsgegevens waarborgen de juistheid en volledigheid van persoonsgegevens		
Fase informatielevenscyclusmanagement: **Inzage en kwaliteit van gegevens**		
Beheersingsmaatregelen:		
ACD01	De entiteit heeft procedures opgesteld om: a. persoonsgegevens aan te passen en te valideren wanneer deze worden verzameld, gecreëerd, bijgehouden en bijgewerkt; b. de datum vast te leggen waarop de persoonsgegevens zijn verkregen of bijgewerkt; c. te specificeren wanneer de persoonsgegevens niet meer geldig zijn; d. te specificeren wanneer en hoe de persoonsgegevens dienen te worden bijgewerkt en wat de bron voor de bijwerking is (bijvoorbeeld een jaarlijkse herbevestiging van de beschikbare informatie en methoden om persoonsgegevens proactief te laten bijwerken door betrokkenen); e. de juistheid en volledigheid te verifiëren van persoonsgegevens die zijn verkregen van de betrokkene of van derden, of die zijn verstrekt aan derden; f. te waarborgen dat de verwerkte persoonsgegevens juist en volledig genoeg zijn om beslissingen op te baseren.	VV
ACD02	De entiteit voert periodiek beoordelingen uit om de juistheid van persoonsgegevens te controleren en deze zo nodig te corrigeren, teneinde het betreffende doel te verwezenlijken.	VV
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking		

Verstrekken

Verstrekking aan derden en registratie (TPD) *Beheersingsdoelstelling:* Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis of voor andere doeleinden dan waarover de betrokkene is geïnformeerd.		
Fase informatielevenscyclusmanagement: **Verstrekken**		
Beheersingsmaatregelen:		
TPD01	De entiteit heeft procedures ingericht om: a. te voorkomen dat persoonsgegevens aan derden worden verstrekt, terwijl de wettelijke basis daarvoor ontbreekt en/of de betrokkene daarover niet is geïnformeerd; b. te documenteren wat de aard van de persoonsgegevens is die aan derden worden verstrekt en in welke mate deze worden verstrekt; c. te monitoren of de verstrekking aan derden nog steeds in overeenstemming is met het privacybeleid en de privacyprocedures van de entiteit, of uitdrukkelijk is toegestaan of verplicht is op grond van wet- of regelgeving; d. te documenteren of persoonsgegevens aan derden worden verstrekt om juridische redenen; e. betrokkenen te informeren en hun toestemming te verkrijgen om persoonsgegevens te verstrekken aan derden voor doeleinden die niet in de privacyverklaring staan; f. erop toe te zien dat persoonsgegevens alleen aan derden worden verstrekt voor de doeleinden in de privacyverklaring.	VV
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Rechtmatigheid van de verwerking		

Overeenkomsten met derden (TPA) *Beheersingsdoelstelling:* Bij de verwerving van oplossingen en diensten (gerelateerd aan persoonsgegevens) van derden wordt voldoende aandacht besteed aan privacyoverwegingen en -vereisten, waardoor op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd.		
Fase informatielevenscyclusmanagement: **Verstrekken**		
Beheersingsmaatregelen:		
TPA01	(a) Indien de entiteit oplossingen van derden/leveranciers verwerft of processen aan dienstverleners uitbesteedt en de verwerking van persoonsgegevens (gedeeltelijk) extern plaatsvindt, gaat de entiteit formele overeenkomsten aan die de derden ertoe verplichten de nodige zorgvuldigheid te betrachten en een beschermingsniveau te waarborgen dat gelijk is aan dat van de entiteit. Op deze wijze beperkt de entiteit het gebruik van persoonsgegevens door derden tot de door de entiteit vastgestelde doeleinden. (b) De entiteit zorgt dat het (verder) uitbesteden van de verwerking van persoonsgegevens slechts plaatsvindt na goedkeuring daarvan door de verwerkingsverantwoordelijke. Indien die toestemming wordt verleend, gaat de entiteit formele overeenkomsten aan die de derde partij ertoe verplichten de nodige zorgvuldigheid te betrachten en een beschermingsniveau te waarborgen dat gelijk is aan dat van de entiteit.	VV V
TPA02	De entiteit zorgt dat in de overeenkomsten eveneens de volgende verplichtingen voor de andere partij zijn opgenomen: a. vertrouwelijkheids- en geheimhouding; b. beveiligingsvereisten; c. medewerking bij het behandelen van verzoeken van betrokkenen en de uitoefening van rechten van de betrokkenen; d. informatieverstrekking (bijv. in het geval van geplande uitbesteding); e. informatieverstrekking en medewerking bij inbreuken in verband met persoonsgegevens; f. bewaartermijnen en verwijdering van gegevens; g. geen verdere uitbesteding zonder toestemming van de entiteit; h. aansprakelijkheid en vrijwaring.	VV, V

TPA03	De entiteit evalueert de prestaties en de naleving van de verplichtingen door derden aan de hand van een of meerdere methoden (in oplopende volgorde van zekerheid en afhankelijk van het risicoprofiel van de derde partij): a. de derde partij vult een vragenlijst in over de manier van werken; b. de derde partij beoordeelt zelf of de werkwijzen voldoen aan de vereisten van de entiteit op basis van interne auditrapporten of andere procedures; c. de entiteit voert periodiek een evaluatie op locatie uit bij de derde partij; d. de entiteit laat een audit of assurance assessment uitvoeren door een onafhankelijke auditor.	VV, V
Gerelateerde kernelementen van de AVG: • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker • Beveiliging van de verwerking		

Doorgifte van persoonsgegevens (DTR)		
Beheersingsdoelstelling: Persoonsgegevens worden niet doorgegeven (d.w.z. verplaatst, weergegeven of geprint op een andere locatie) aan landen die geen toereikend rechtskader ten aanzien van privacy hebben.		
Fase informatielevenscyclusmanagement: **Verstrekken**		
Beheersingsmaatregelen:		
DTR01	De entiteit heeft alle gevallen in kaart gebracht waarin persoonsgegevens waar zij de verantwoordelijkheid voor draagt worden doorgegeven aan en verwerkt in derde landen die mogelijk de privacy van betrokkenen niet voldoende waarborgen.	VV, V
DTR02	De entiteit geeft alleen persoonsgegevens door aan derde landen (a) waarvoor de Europese Commissie een adequaatheidsbesluit heeft genomen, of (b) die een set passende waarborgen hebben getroffen (bijv. bindende bedrijfsvoorschriften of standaardbepalingen inzake gegevens-bescherming).	VV, V
Gerelateerde kernelementen van de AVG: • Doorgiften van persoonsgegevens aan derde landen of internationale organisaties		

Gegevensbeveiliging

Programma informatiebeveiliging (ISP)

Beheersingsdoelstelling:

Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde verstrekking of verlies.

Fase informatielevenscyclusmanagement: **Gegevensbeveiliging**

Beheersingsmaatregelen:		
ISP01	De entiteit heeft passende technische en organisatorische maatregelen genomen om de beveiliging van persoonsgegevens te waarborgen. De beveiliging omvat de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens. Zie ook IAM, STR, ENC, LOG.	VV, V
ISP02	De beveiliging van persoonsgegevens komt uitdrukkelijk aan de orde in het beleid van de entiteit voor informatiebeveiliging en het managementsysteem voor informatiebeveiliging.	VV, V
ISP03	In hoeverre de beveiligingsmaatregelen met betrekking tot persoonsgegevens adequaat zijn, wordt bepaald door middel van periodieke risicobeoordelingen waaraan alle relevante belanghebbenden deelnemen en waarbij zowel naar de huidige als de toekomstige verwerkingsactiviteiten wordt gekeken.	VV, V
ISP04	De entiteit heeft een gedocumenteerd beleid ten aanzien van versleuteling en pseudonimisering van persoonsgegevens en verifieert systematisch dat het beleid wordt nageleefd (zie ook ENC).	VV, V
ISP05	De entiteit toetst, beoordeelt en evalueert op regelmatige basis de effectiviteit van de technische en organisatorische beveiligingsmaatregelen om een adequaat beveiligingsniveau te waarborgen en verbeteringen te identificeren en door te voeren.	VV, V
ISP06	De entiteit stelt zich actief op tegenover het gebruik van een gedragscode (van branche- en beroepsverenigingen of sectororganisaties) en/of certificeringen om aan te tonen dat de entiteit een passend beschermingsniveau waarborgt.	VV, V
ISP07	Het beveiligingsprogramma van de entiteit voorkomt dat personen toegang hebben tot persoonsgegevens in computers, media en op papier die niet meer actief door de organisatie worden gebruikt (zoals computers, media en informatie op papier die zijn opgeslagen, verkocht of op andere wijze zijn verwijderd).	VV, V

Gerelateerde kernelementen van de AVG:

- Beveiliging van de verwerking

Identiteit en toegangsbeheer (IAM) *Beheersingsdoelstelling:* Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans opop ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers..		
Fase informatielevenscyclusmanagement: **Gegevensbeveiliging**		
Beheersingsmaatregelen:		
IAM01	De entiteit heeft systemen en procedures ingericht om: a. vast te stellen in hoeverre en op welke wijze gebruikers toegang krijgen tot persoonsgegevens. Dit is gebaseerd op de gevoeligheid van de gegevens en de gerechtvaardigde zakelijke doeleinden van de gebruikers; b. gebruikers te identificeren en te authenticeren (bijvoorbeeld door middel van een gebruikersnaam en wachtwoord, certificaat, extern token of biometrische gegevens) voordat toegang wordt verleend tot systemen die persoonsgegevens verwerken; c. strengere beveiligingsmaatregelen in te stellen voor toegang op afstand, zoals extra of dynamische wachtwoorden, callback-procedures, digitale certificaten, beveiligde ID-kaarten, virtual private network (VPN), of adequaat geconfigureerde firewalls; d. toegangsdetectie en monitoringssystemen te implementeren.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking		

Veilige gegevensoverdracht (STR) *Beheersingsdoelstelling:* Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen.		
Fase informatielevenscyclusmanagement: **Gegevensbeveiliging**		
Beheersingsmaatregelen:		
STR01	De entiteit heeft systemen en procedures ingericht om: a. het minimumniveau van beveiliging vast te stellen voor verzending van persoonsgegevens; b. bij het doorgeven en ontvangen van persoonsgegevens versleutelingstechnologie toe te passen die de standaard is in de sector; c. externe netwerkverbindingen te beoordelen en goed te keuren; d. persoonsgegevens te beschermen in zowel gedrukte als elektronische vorm, verstuurd per post, koerier of andere fysieke methode; e. via draadloze netwerken verzamelde en verzonden persoonsgegevens te versleutelen en draadloze netwerken te beschermen tegen ongeautoriseerde toegang.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Inbreuk in verband met persoonsgegevens		

Versleuteling en eindpuntbeveiliging (ENC) *Beheersingsdoelstelling:* Inbreuk in verband met persoonsgegevens (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) wordt voorkomen door middel van versleuteling.		
Fase informatielevenscyclusmanagement: **Gegevensbeveiliging**		
Beheersingsmaatregelen:		
ENC01	Beleidsregels en procedures verbieden de opslag van persoonsgegevens op draagbare media of apparaten, tenzij er sprake is van zakelijke noodzaak en de opslag is goedgekeurd door het management.	VV, V
ENC02	De entiteit heeft beleid, systemen en procedures opgesteld om persoonsgegevens te beschermen die toegankelijk zijn via of zijn opgeslagen op de volgende apparaten: a. laptops, pda's, smartphones en vergelijkbare apparaten; b. computers en andere apparaten die medewerkers gebruiken als zij bijvoorbeeld onderweg zijn of vanuit huis werken; c. USB-sticks, cd's, dvd's, magneetband en andere draagbare media. Dergelijke informatie wordt versleuteld, beveiligd met een wachtwoord en fysiek beschermd, en hierop is het toegangs-, bewaar- en vernietigingsbeleid van de entiteit van toepassing.	VV, V
ENC03	De entiteit heeft procedures en systemen voor het creëren, verplaatsen, opslaan en verwijderen van media met persoonsgegevens die zijn gebruikt voor back-ups en herstel.	VV, V
ENC04	De entiteit heeft procedures voor het rapporteren van mogelijk misbruik van media met persoonsgegevens (zie ook PIA). Wanneer het dienstverband van medewerkers of overeenkomsten met derden worden beëindigd, zijn er procedures voor het terughalen en vernietigen van draagbare media en apparaten die gebruikt zijn om toegang te verkrijgen tot persoonsgegevens of deze op te slaan. Dit geldt eveneens voor geprinte informatie en andere bestaande kopieën.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Inbreuk in verband met persoonsgegevens		

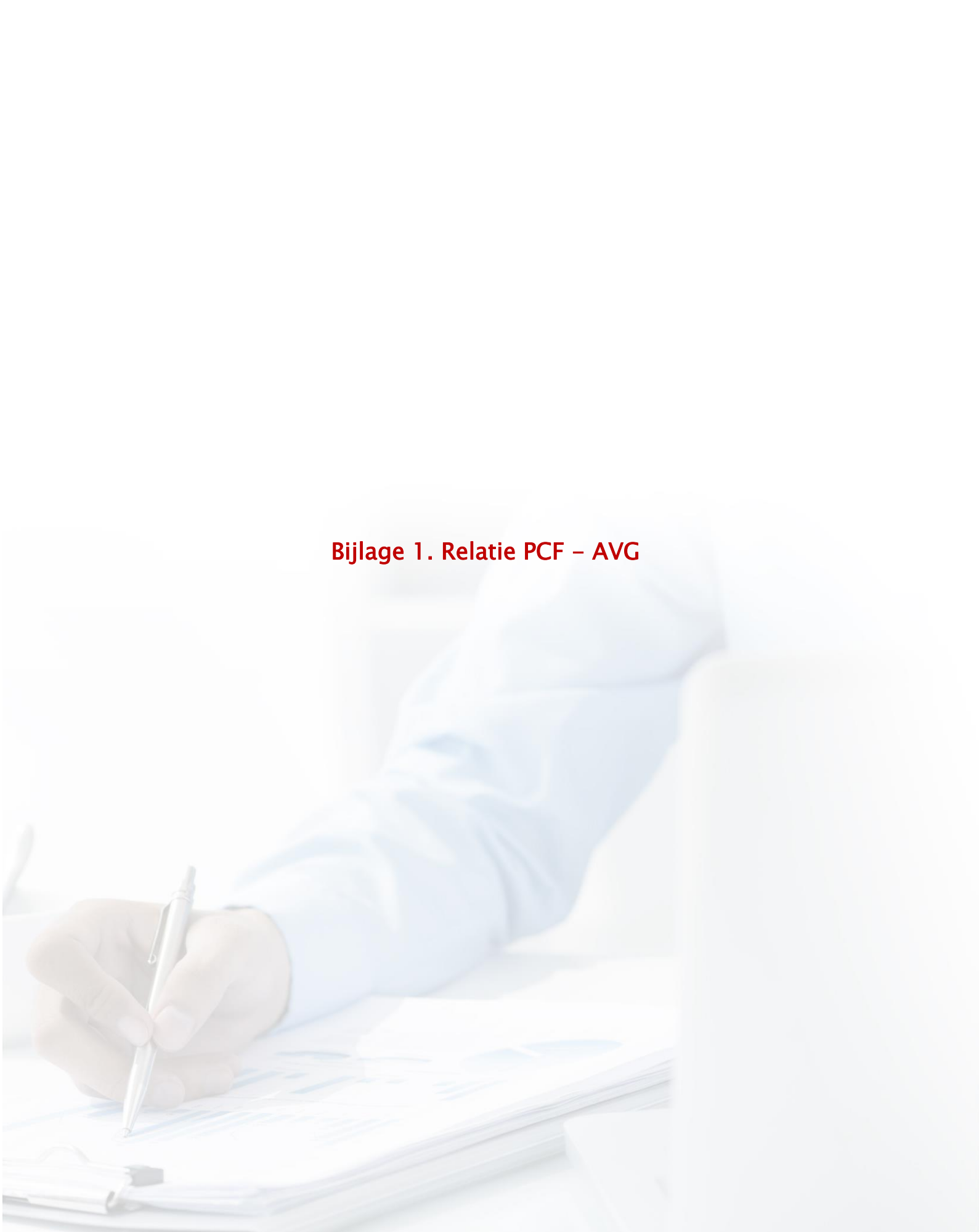
Registreren van toegang (LOG) *Beheersingsdoelstelling:* Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen.		
Fase informatielevenscyclusmanagement: **Gegevensbeveiliging**		
Beheersingsmaatregelen:		
LOG01	De entiteit heeft systemen en procedures ingericht om: a. de logische en fysieke toegang tot persoonsgegevens te beheren, inclusief hardcopy's, archiefkopieën en back-upkopieën; b. de toegang tot systemen met persoonsgegevens (of pogingen hiertoe) te registreren en te monitoren. De logbestanden bevat voldoende details en wordt lang genoeg bewaard om de gegevens te kunnen analyseren en onderzoeken; c. het ongeautoriseerd of onopzettelijk vernietigen of verliezen van persoonsgegevens te voorkomen; d. inbreuken in verband met persoonsgegevens en pogingen om ongeautoriseerde toegang te verkrijgen te onderzoeken.	VV, V
Gerelateerde kernelementen van de AVG: • Beveiliging van de verwerking • Inbreuk in verband met persoonsgegevens		

Monitoren en handhaven

Beoordeling van naleving privacywetgeving (REV) *Beheersingsdoelstelling:* Adequaat toezicht op de interne organisatie en derden waarborgt dat de entiteit voldoet aan de wet- en regelgeving met betrekking tot privacy en vermindert het risico op inbreuk in verband met persoonsgegevens of verlies hiervan..		
Fase informatielevenscyclusmanagement: **Monitoren en handhaven**		
Beheersingsmaatregelen:		
REV01	De entiteit heeft systemen en procedures ingericht om: a. jaarlijks de naleving te beoordelen van privacybeleid en -procedures, verplichtingen en geldende wet- en regelgeving, Service Level Agreements, door de entiteit opgestelde normen en andere overeenkomsten; b. periodiek beoordelingen te documenteren, zoals, interne auditplannen, auditrapporten, compliance checklists en aftekeningen ('sign-offs') van het management; c. de resultaten van de conformiteitsbeoordeling en aanbevelingen voor verbetering aan het management te rapporteren, en een verbeterplan te implementeren; d. de oplossing van problemen en de kwetsbaarheden die naar voren komen in de conformiteitsbeoordeling te monitoren, om te waarborgen dat tijdig passende corrigerende maatregelen worden genomen (waaronder herziening van het privacybeleid en procedures, indien nodig).	VV, V
Gerelateerde kernelementen van de AVG: • Rechtmatigheid van de verwerking		

Periodiek monitoren van privacybeheersingsmaatregelen (MON)		
Beheersingsdoelstelling: Systematische en periodieke evaluatie van privacyprocessen en beheersingsmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving.		
Fase informatielevenscyclusmanagement: **Monitoren en handhaven**		
Beheersingsmaatregelen:		
MON01	Het management van de entiteit evalueert de volgende zaken om de werking van privacybeheersingsmaatregelen te waarborgen: a. control outputs, controlerapporten en deviaties; b. trendanalyse; c. aanwezigheid bij trainingen en evaluaties; d. klachten en oplossing daarvan; e. interne beoordelingen; f. interne en externe auditrapporten; g. onafhankelijke audit/assurance-rapporten met betrekking tot privacybeheersingsmaatregelen bij dienstverlenende organisaties; h. andere informatie met betrekking tot de doeltreffendheid van de beheersingsmaatregelen.	VV, V
MON02	De entiteit beslist op basis van de gevoeligheid van de betreffende persoonsgegevens en het risico op blootstelling of verlies welke beheersingsmaatregelen worden gemonitord, beoordeeld en/of gecontroleerd, hoe en met welke frequentie dit gebeurt .	VV, V
MON03	De entiteit heeft een proces ingericht om te waarborgen dat het monitoren resulteert in herstel van tekortkomingen en continue verbetering.	VV, V
Gerelateerde kernelementen van de AVG: • Rechtmatigheid van de verwerking		

Bijlage 1. Relatie PCF – AVG



Relatie tussen kernelementen AVG en artikelen AVG

De onderstaande tabel geeft inzicht in de relatie tussen kernelementen van de AVG, de betreffende artikelen in de wet, en de topics uit het PCF.

AVG Kernelement	Gerelateerde AVG artikelen	Cross-reference met PCF topics
Privacyprincipes	Artikel 5 – Beginselen inzake verwerking van persoonsgegevens	• Privacybeleid (PPO) • Afbakening van rollen en verantwoordelijk-heden (RRE) • Competenties medewerkers (SCO) • Identificatie en classificatie van persoonsgegevens (PDI) • Bewustwording en training medewerkers (SAT) • Doelbinding (ULI) • Privacyverklaring (PST) • Minimale gegevensverwerking (DMI) • Doelbinding (ULI) • Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) • Bewaren van gegevens (DRE) • Verwijdering, vernietiging en anonimisatie (DDA) • Gebruik en beperking (URE)
Rechtmatigheid van de verwerking	Artikel 6 – Rechtmatigheid van de verwerking	• Privacybeleid (PPO) • Toestemmingsraamwerk (CFR) • Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC) • Gebruik en beperking (URE) • Verstrekking aan derden en registratie (TPD) • Beoordeling van naleving privacywetgeving (REV)

AVG Kernelement	Gerelateerde AVG artikelen	Cross-reference met PCF topics
		• Periodiek monitoren van privacy-beheersingsmaatregelen (MON)
Voorwaarden voor toestemming	Artikel 7 – Voorwaarden voor toestemming	• Privacybeleid (PPO) • Toestemmingsraamwerk (CFR) • Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC) • Gebruik en beperking (URE) • Verstrekking aan derden en registratie (TPD) • Beoordeling van naleving privacywetgeving (REV) • Periodiek monitoren van privacy-beheersings-maatregelen (MON)
Rechten van de betrokkene	Artikel 12 – Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene Artikel 13 – Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld Artikel 14 – Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen Artikel 15 – Recht van inzage van de betrokkene Artikel 16 – Recht op rectificatie Artikel 17 – Recht op gegevenswissing ('recht op vergetelheid') Artikel 18 – Recht op beperking van de verwerking Artikel 19 – Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking Artikel 20 – Recht op overdraagbaarheid van gegevens	• Gebruik en beperking (URE) • Verzoek tot inzage (DAR) • Toestemmingsraamwerk (CFR) • Privacyverklaring (PST) • Verzoek tot rectificatie (DCR) • Verzoek tot wissen (DDR)

AVG Kernelement	Gerelateerde AVG artikelen	Cross-reference met PCF topics
Recht op overdraagbaarheid van gegevens	Artikel 20 – Recht op overdraagbaarheid van gegevens	• Verzoek tot overdracht (DPR)
Gegevensbescherming door ontwerp / door standaardinstellingen	Artikel 25 – Gegevensbescherming door ontwerp en door standaardinstellingen	• Risicomanagement (RMA) • Afbakening van rollen en verantwoordelijkheden (RRE) • Competenties medewerkers (SCO) • Minimale gegevensverwerking (DMI) • Doelbinding (ULI) • Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) (PBD) • Verzoek tot inzage (DAR) • Verwijdering, vernietiging en anonimisatie (DDA)
Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker	Artikel 24 – Verantwoordelijkheid van de verwerkingsverantwoordelijke Artikel 28 – Verwerker	• Afbakening van rollen en verantwoordelijkheden (RRE) • Privacyverklaring (PST) • Bewaren van gegevens (DRE) • Verwijdering, vernietiging en anonimisatie (DDA) • Overeenkomsten met derden (TPA)
Register van de verwerkingsactiviteiten	Artikel 30 – Register van de verwerkingsactiviteiten	• Privacybeleid (PPO) • Afbakening van rollen en verantwoordelijkheden (RRE) • Identificatie en classificatie van persoonsgegevens (PDI)
Beveiliging van de verwerking	Artikel 32 – Beveiliging van de verwerking	• Identificatie en classificatie van persoonsgegevens (PDI) • Competenties medewerkers (SCO) • Bewustwording en training medewerkers (SAT)

AVG Kernelement	Gerelateerde AVG artikelen	Cross-reference met PCF topics
		• Afbakening van rollen en verantwoordelijkheden (RRE) • Verwijdering, vernietiging en anonimisatie (DDA) • Verzoek tot inzage (DAR) • Juistheid en volledigheid van gegevens (ACD) • Verstrekking aan derden en registratie (TPD) • Overeenkomsten met derden (TPA) • Programma informatiebeveiliging (ISP) • Identiteit en toegangsbeheer (IAM) • Veilige gegevens-overdracht (STR) • Versleuteling en eindpuntbeveiliging (ENC) • Registreren van toegang (LOG)
Inbreuk in verband met persoonsgegevens	Artikel 33 – Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit Artikel 34 – Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene	• Beheer van privacyincidenten en inbreuken (PIB) • Veilige gegevensoverdracht (STR) • Versleuteling en eindpuntbeveiliging (ENC) • Registreren van toegang (LOG)
Gegevensbeschermingseffectbeoordelingen (PIA)	Artikel 35 – Gegevensbeschermings-effectbeoordeling	• Risico-management (RMA) • Data protection impact assessments(PIA) • Juridische beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC)
Functionaris voor gegevensbescherming (FG)	Artikel 37 – Aanwijzing van de functionaris voor gegevensbescherming Artikel 38 – Positie van de functionaris voor gegevensbescherming Artikel 39 – Taken van de functionaris voor gegevensbescherming	• Afbakening van rollen en verantwoordelijkheden (RRE) • Competenties medewerkers (SCO)

AVG Kernelement	Gerelateerde AVG artikelen	Cross-reference met PCF topics
Doorgiften van persoonsgegevens aan derde landen of internationale organisaties	Artikel 44 – Algemeen beginsel inzake doorgiften Artikel 45 – Doorgiften op basis van passende waarborgen Artikel 46 – Transfers subject to appropriate safeguards Artikel 47 – Bindende bedrijfsvoorschriften Artikel 48 – Niet bij Unierecht toegestane doorgiften of verstrekkingen Artikel 49 – Afwijkingen voor specifieke situaties Artikel 50 – Internationale samenwerking voor de bescherming van persoonsgegevens	• Afbakening van rollen en verantwoordelijkheden (RRE) • Gebruik en beperking (URE) • Doorgifte van persoonsgegevens (DTR)

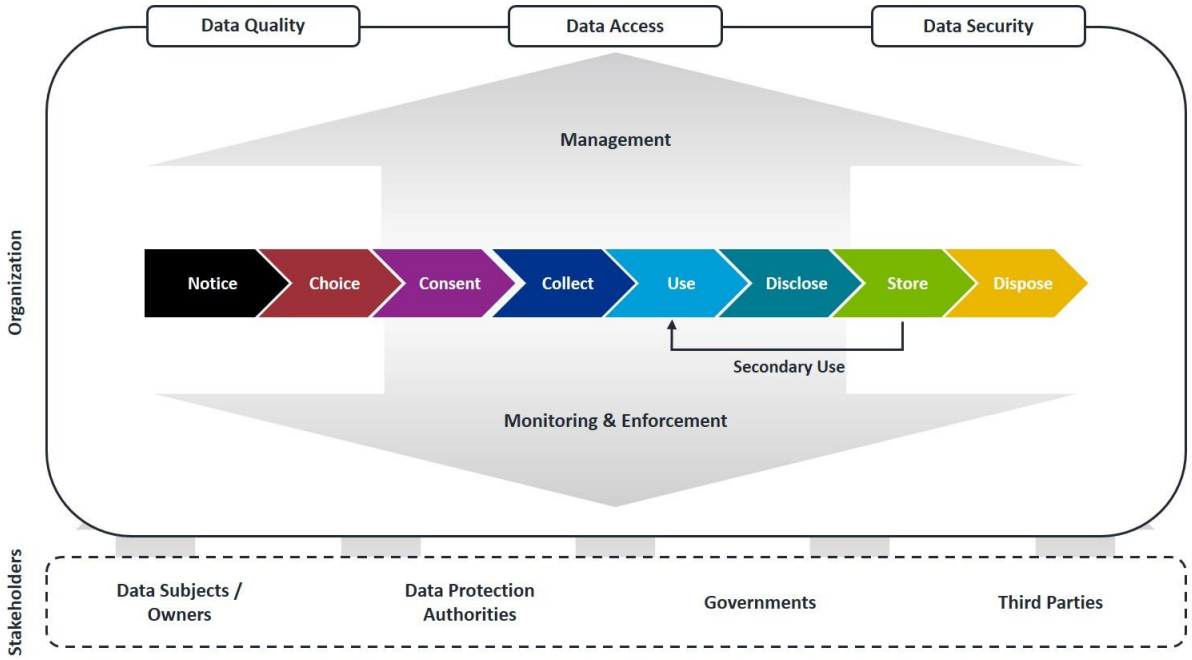
Bijlage 2. Informatielevenscyclus

Inleiding

In deze bijlage wordt in hoofdlijnen het informatielevenscyclusmodel zoals beschreven in deel 1 – Introductie toegelicht.

Het PCF is gestructureerd volgens een informatielevenscyclusmodel dat voor het eerst beschreven werd in de scriptie van Koetsier en Ougajou en de daaropvolgende publicatie in *de IT-Auditor*.

Het volgende figuur is een grafische weergave van het informatielevenscyclusmodel:



Figuur 1 Informatielevenscyclusmodel

De verschillende fasen

Het informatielevenscyclusmodel is gebaseerd op en opgebouwd uit een combinatie van de GAPP[6]-principes en de OECD[7]-richtlijnen. Het informatielevenscyclusmodel bestaat uit 8 verschillende fasen:

1. **Informeren**: De informatielevenscyclus begint met het informeren van de betrokkene over het gebruik van diens persoonsgegevens. De entiteit maakt het privacybeleid en de procedures kenbaar en geeft aan voor welke doeleinden de persoonsgegevens worden verzameld, gebruikt, bewaard en verstrekt.

2. **Keuze**: De entiteit geeft aan welke opties de betrokkene heeft met betrekking tot de verzameling, het gebruik en de verstrekking van persoonsgegevens door de entiteit.

3. **Toestemming**: De entiteit verkrijgt stilzwijgende of uitdrukkelijke toestemming van de betrokkene ten aanzien van de verzameling, het gebruik en de verstrekking van de persoonsgegevens.

4. **Verzamelen**: De entiteit verzamelt de persoonsgegevens enkel voor de doeleinden omschreven in de fase Informeren.

5. **Gebruiken**: De entiteit gebruikt de persoonsgegevens enkel voor de doeleinden omschreven in de fase Informeren en waarvoor de betrokkene stilzwijgend of uitdrukkelijk toestemming heeft gegeven.

6. **Verstrekken**: De entiteit verstrekt de persoonsgegevens enkel aan derden voor de doeleinden omschreven in de fase Informeren en met de stilzwijgende of uitdrukkelijke toestemming van de betrokkene.

7. **Opslaan**: De entiteit bewaart persoonsgegevens niet langer dan nodig is voor het doel omschreven in de fase Informeren of dan wettelijk is vastgesteld. Het is mogelijk dat persoonsgegevens opnieuw worden gebruikt (secundair gebruik) en weer de fase Gebruiken ingaan, maar dit mag alleen als de doeleinden voor secundair gebruik in overeenstemming zijn met de doeleinden omschreven in de fase Informeren.

8. **Verwijderen**: De entiteit verwijdert persoonsgegevens op de juiste wijze.

[6] GAPP, An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009

[7] The OECD Privacy Framework, Organisation for Economic Co-operation and Development, 2013

Randvoorwaarden - management en belanghebbenden

Het management bepaalt de koers (privacystrategie, privacybeleid, etc.) en ziet erop toe dat persoonsgegevens op gecontroleerde wijze de verschillende fasen van de informatielevenscyclus doorlopen (monitoren en handhaven). In het algemeen zijn er in de fasen drie randvoorwaarden voor persoonsgegevens om te waarborgen dat bedrijfsprocessen tijdig en op accurate en volledige wijze worden uitgevoerd:

- Kwaliteit van gegevens;
- Inzage van gegevens;
- Gegevensbeveiliging

Tot slot worden in het informatielevenscyclusmodel de verschillende externe belanghebbenden weergegeven die bij de verwerkingsfasen van persoonsgegevens betrokken zijn. Deze belanghebbenden zijn:

- Betrokkenen;
- Gegevensbeschermingsautoriteiten (zoals de Autoriteit Persoonsgegevens in Nederland);
- Overheden;
- Derden (of verwerkers).

Op basis van dit conceptuele model is het PCF ontwikkeld. Dit raamwerk omvat een overzicht van beheersingsdoelstellingen en bijbehorende beheersingsmaatregelen. De beheersingsdoelstellingen zijn gegroepeerd op basis van de fasen in het informatielevenscyclusmodel.

Op deze wijze is duidelijk welke privacybeheersingsdoelstellingen in welke fase van het informatielevenscyclusmodel aan bod komen. Entiteiten kunnen met behulp van dit model het beheer van persoonsgegevens sterk verbeteren.

Bijlage 3. PCF en ISO standaarden

Deze bijlage geeft enige verduidelijking aan de relatie tussen het PCF en:

- ISO 27001/27002 (waaraan in deze bijlage gemakshalve gerefereerd wordt als 'ISO 27001')[8]
- ISO 27701
- ISO 29100

ISO 27001 en privacy

De woorden 'privacy' en 'persoonsgegevens' komen in ISO 27001 slechts sporadisch voor. Dat hoeft geen verbazing te wekken want de norm is gericht op beveiliging van informatie in zijn algemeenheid, waarbij wel rekening moet worden gehouden met de aard en classificatie van gegevens. Persoonsgegevens zijn daarmee impliciet in ISO 27001 ingesloten. In de beheersmaatregelen van ISO 27001 worden persoonsgegevens slechts op een enkele plek expliciet genoemd. In A.18.1.4 (in het hoofdstuk "Naleving" van bijlage A) van de norm staat als doelstelling:

"Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving."

Welbeschouwd verplicht ISO 27001 dus tot afdoende bescherming van persoonsgegevens én compliance met de AVG. In deze lijn van redenering zou kunnen worden verdedigd dat voldoen aan de eisen van ISO 27001 ook garant staat voor afdoende maatregelen op het gebied van de bescherming van persoonsgegevens en voldoen aan privacygerelateerde wet- en regelgeving. In theorie kan het PCF worden gebruikt om een adequate opzet en implementatie van norm A.18.1.4 vast te stellen. De praktische uitvoerbaarheid daarvan is twijfelachtig. Aan ISO 27001 worden dan 32 beheersdoelstellingen uit het PCF 'toegevoegd' om vast te stellen of één van de doelstellingen van ISO 27001 wordt gehaald.

Een praktischer wijze van co-existentie van ISO 27001 en PCF is om privacygerelateerde beheersmaatregelen te zien als een 'verbijzondering voor persoonsgegevens' van meerdere individuele voorgeschreven beheersmaatregelen uit ISO 27001. Hiermee wordt het PCF als het ware 'uitgesmeerd' over ISO 27001 en niet opgehangen aan de individuele norm A.18.1.4. Professionals hanteren dan het PCF als een privacygerelateerd addendum bovenop ISO 27001, waarbij rekening wordt gehouden met persoonsgegevens als een bijzondere vorm van informatie die eisen stelt die

[8] NEN-ISO/IEC 27001 is een informatiebeveiligingsstandaard die de vereisten specificeert voor een beheersingssysteem van informatiebeveiliging ('information security management system', ISMS). ISO/IEC 27002 geeft best practices voor ontwerp en implementatie van een ISMS, uitgaande van dezelfde doelstellingen als ISO 27001.

verbijzonderingen zijn van de bestaande ISO 27001-eisen. Om dit te illustreren is hieronder het voorbeeld genomen van ISO 27001 A.16 (Beheer van Informatiebeveiligingsincidenten), dat wordt gekoppeld met PCF PIB (Privacy Incident and breach Management).

	ISO 27001 – ISMS	PCF – Privacyspecifiek
Topic/onderdeel	**A.16** Beheer van informatiebeveiligingsincidenten	**PIB** – Beheer van privacyincidenten en inbreuken
Beheerdoelstelling	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	De entiteit detecteert incidenten met betrekking tot privacy en handelt deze af. Op privacy-gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken en er worden maatregelen genomen om inbreuk in de toekomst te voorkomen.
Beheersmaatregel	**A.16.1.2** Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	**PIB03** Het proces bevat een duidelijke escalatieprocedure, gebaseerd op het type en/of de ernst van het incident, tot aan het inwinnen van juridisch advies en het inlichten van het hoogste management. In de procedure staan de criteria voor het opnemen van contact met rechtshand-havende-, toezichthoudende of andere autoriteiten.

Bij een dergelijke aanpak is het handig om te beschikken over een 'mapping' van beheersmaatregelen uit ISO 27001 met beheersmaatregelen uit het PCF (in analogie met wat in bovenstaand voorbeeld is gedaan voor A.16.1.2 (ISO 27001) en PIB03 (PCF). Deze (indicatieve) mapping is opgenomen in de tabel aan het einde van deze bijlage, als ondersteuning van beroepsbeoefenaren die het PCF hanteren in een entiteit waar ISO 27001 voor informatiebeveiliging al normatief wordt gebruikt.

ISO 27701

Ook ISO lijkt een soortgelijke aanpak als hierboven beschreven voor te staan. Zij heeft begin augustus 2019 ISO/IEC 27701:2019 (kortweg ISO 27701) gepubliceerd, dat een (privacy-)uitbreiding is op de eisen en richtlijnen van respectievelijk ISO 27001 en ISO 27002. De volledige titel van de norm is 'Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.'

Kort samengevat geeft ISO 27701 privacy-aanvullingen en verfijningen op de bestaande clausules en eisen uit ISO 27001 en op de richtlijnen ('guidance') uit ISO 27002. Waar ISO 27001 en ISO 27002 zich richten op (eisen aan) een managementsysteem voor informatiebeveiliging (ISMS), breidt ISO 27701 dit in feite uit met eisen ten aanzien van een managementsysteem voor persoonsgegevens (Privacy Information Management System, PIMS). Op basis van ISO 27701 kan dus ook het PIMS van een organisatie worden ontworpen, geïmplementeerd en gecertificeerd. In één van de bijlages bij ISO 27701 is een uitgebreide referentie opgenomen van de eisen uit ISO 27701 met de relevante artikelen uit de AVG.

ISO 29100

Om het beeld te completeren zij opgemerkt dat er een additionele ISO-standaard is die specifiek is gericht op privacy. Dat is ISO/IEC 29100:2011 (kortweg ISO 29100) met de titel "Information technology - Security techniques - Privacy framework". Deze standaard geeft de contouren van een privacyraamwerk op hoog niveau, waardoor organisaties in staat worden gesteld om:

- een gemeenschappelijke privacy-terminologie te hanteren;
- te definiëren welke actoren in de verwerking van persoonsgegevens een rol spelen en wat hun verantwoordelijkheden zijn;
- privacybeschermingsmaatregelen te beschrijven;
- te refereren aan bekende privacyprincipes.

In termen van privacybeschermingsmaatregelen is ISO 29100 tamelijk algemeen geformuleerd, en als een basis te beschouwen voor de nadere uitwerking in ISO 27701.

Cross-reference tussen PCF en ISO

In onderstaande tabel is een indicatieve cross-reference gemaakt van de onderwerpen uit het PCF met de bovengenoemde ISO standaarden.

Tag (PCF)	Topic (PCF)	Gerelateerde eisen en beheersings-maatregelen ISO 27001:2013	Gerelateerde beheersmaatregelen ISO 27701:2019	Gerelateerde principes ISO 29100:2011
PPO	Privacybeleid	A.5.1.1, A.5.1.2, A.18.1.3, A.18.1.4 Clause: 5.2	A.7.2.1, A.7.2.2, A.7.3.1, A.7.3.10, B.8.2.1, B.8.2.6	Purpose legitimacy and specification Openness, transparency and notice Accountability
RRE	Afbakening van rollen en verantwoordelijkheden	A.6.1.1, A.7.1.2, A.7.2.1, A.15.1.1, A.15.1.2, A.15.1.3 Clause: 5.1, 5.3	5.2.1 A.7.2.7, B.8.2.1, B.8.2.6	Accountability
PDI	Identificatie en classificatie van persoonsgegevens	A.8.1.1, A.8.2.1, A.8.2.2, A.8.2.3	A.7.2.1, A.7.2.2, A.7.2.8, A.7.3.10, B.8.2.2	Purpose legitimacy and specification
RMA	Risicomanagement	A.5.1.2 Clause: 6.1.1, 6.1.2, 6.1.3, 8.2	5.4.1.2	Accountability
PIA	Data protection impact assessments	A.5.1.2, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.5 Clause: 6.1.2, 6.1.3, 8.2	5.4.1.2 A.7.2.5	Accountability
PIB	Beheer van privacyincidenten en inbreuken	A.16.1.1 t/m A.16.1.7		Accountability
SCO	Competenties medewerkers	Clause: 7.2		Accountability
SAT	Bewustwording en training medewerkers	A.7.2.2 Clause: 7.3		Accountability

Tag (PCF)	Topic (PCF)	Gerelateerde eisen en beheersings-maatre-gelen ISO 27001:2013	Gerelateerde be-heersmaatregelen ISO 27701:2019	Gerelateerde principes ISO 29100:2011
LRC	Juridische toets van wijzigingen in wet- en regel-geving en/of bedrijfsvereisten	A.18.1.1 Clause: 4.2		Privacy compliance
PST	Privacyverklaring	–	A.7.3.1, A.7.3.2, A.7.3.3	Openness, transparency and notice
CFR	Toestemmings-raamwerk	–	A.7.2.3, A.7.2.4, A.7.3.4	Consent and choice
DMI	Minimale gegevens-verwerking	–	A.7.4.1, A.7.4.2, A.7.4.4	Data minimisation / Collection limitation
ULI	Doelbinding	–	A.7.4.1, A.7.4.2	Purpose legitimacy and specification
PBD	Privacyarchitec-tuur (Gegevens-bescherming door ontwerp en door standaard-instellingen)	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.5	A.7.4	Use, retention and disclosure limitation
DRE	Bewaren van gegevens	–	A..7.4.7	Use, retention and disclosure limitation
DDA	Verwijdering, vernietiging en anonimiseren	A.8.3.1, A.8.3.2, A.11.2.7	A.7.4.5, A.7.4.8	Use, retention and disclosure limitation
URE	Gebruik en beperking	–	A.7.3.5	Use, retention and disclosure limitation
DAR	Verzoek tot in-zage	–	A.7.3.3, A.7.3.6, A.7.3.7, A.7.3.8, A.7.3.9	Individual participation and access

Tag (PCF)	Topic (PCF)	Gerelateerde eisen en beheersings-maatregelen ISO 27001:2013	Gerelateerde beheersmaatregelen ISO 27701:2019	Gerelateerde principes ISO 29100:2011
DCR	Verzoek tot rectificatie	–	A.7.3.6, A.7.3.7, A.7.3.9	Individual participation and access / Accuracy and quality
DDR	Verzoek tot wissen	A.8.3.1, A.8.3.2, A.11.2.7	A.7.3.6, A.7.3.7, A.7.3.9, B.8.4.2	Individual participation and access
DPR	Verzoek tot overdracht	A.8.3.3	A.7.3.9	Individual participation and access
ACD	Juistheid en volledigheid van gegevens	–	A.7.4.3	Accuracy and quality
TPD	Verstrekking aan derden en registratie	A.8.3.3	A.7.5.1, A.7.5.3, A.7.5.4	Use limitation
TPA	Overeenkomsten met derden	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	A.7.2.6, B.8.2.5, B.8.3.1, B.8.5.6, B.8.5.7, B.8.5.8	Accountability
DTR	Doorgifte van persoonsgegevens	–	A.7.5.1, A.7.5.2, A.7.5.3, B.8.5.1, B.8.5.2	Accountability
ISP	Programma informatiebeveiliging	A.5.1.1, A.8.3.2, A.10.1.1, A.18.2.2, A.18.2.3		Information security
IAM	Identiteit en toegangsbeheer	A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2		Information security
STR	Veilige gegevensoverdracht	A.10.1.1, A.13.1.1, A.13.1.2, A.13.1.3	A.7.4.9, B.8.4.3	Information security
ENC	Versleuteling en eindpuntbeveiliging	A.8.1.4, A.8.3.1, A.8.3.2, A.10.1.1		Information security

Tag (PCF)	Topic (PCF)	Gerelateerde eisen en beheersings-maatre-gelen ISO 27001:2013	Gerelateerde be-heersmaatregelen ISO 27701:2019	Gerelateerde principes ISO 29100:2011
LOG	Registreren van toegang	A.12.4.1		Information security
REV	Beoordeling van compliance met privacywetgeving	Clause: 9, 10 A.18.1.1, A.18.1.4		Privacy compliance
MON	Periodiek monitoren van privacybeheer-singsmaatregelen	Clause 9, 10 A.18.2.1, A.18.2.2, A.18.2.3		Privacy compliance

In onderstaande tabel is volledigheidshalve en indicatief weergegeven welke privacyonderwerpen uit het PCF bij welke onderdelen van ISO 27001 horen.

Relatie tussen ISO 27001, ISO 27002 en PCF onderwerpen		
ISO 27001:2013	**Onderwerp**	**PCF**
Clause 4	Context van de organisatie	LRC
Clause 5	Leiderschap	PPO, DDR
Clause 6	Planning	RMA
Clause 7	Ondersteuning	SCO
Clause 8	Uitvoering	RMA, PIA
Clause 9	Evaluatie van de prestaties	REV, MON
Clause 10	Verbetering	REV, MON
A.5	Informatiebeveiligingsbeleid	PPO, RMA, PIA, ISP
A.6	Organiseren van in-formatiebeveiliging	RRE, PIA, PBD
A.7	Veilig personeel	RRE, SAT
A.8	Beheer van bedrijfsmiddelen	PDI, DDA, DDR, DPR, TPD, ISP, ENC

A.9	Toegangsbeveiliging	IAM
A.10	Cryptografie	ISP, STR, ENC
A.11	Fysieke beveiliging en beveiliging van de omgeving	DDA, DDR
A.12	Beveiliging Bedrijfsvoering	LOG
A.13	Communicatiebeveiliging	STR
A.14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	PIA, PBD
A.15	Leveranciersrelaties	RRE, TPA
A.16	Beheer van informatie beveiligingsincidenten	PIB
A.17	Informatiebeveiligingsaspecten van bedrijfscontinuiteit	
A.18	Naleving	PPO, LRC, ISP, REV, MON
ISO 27701:2019	**Onderwerp**	**PCF**
A.7.2	Conditions for collection and processing	PPO, PDI, CFR, PIA, TPA, RRE,
A.7.3	Obligations to PII principals	PPO, PDI, PST, CFR, URE, DAR, DCR, DDR, DPR,
A.7.4	Privacy by design and default	DMI, ULI, ACD, DDA, DRE, STR
A.7.5	PII Sharing, transfer and disclosure	TPD, DTR
B.8.2	Conditions for collecting and processing	PPO, RRE, PDI, TPA
B.8.3	Obligations to PII principals	TPA
B.8.4	Privacy by design and default	DDR, STR
B.8.5	PII Sharing, transfer and disclosure	DTR, TPA