

NOREA Handreiking

Privacy Control Framework

Beheersingsdoelstellingen

en beheersingsmaatregelen

voor privacyaudits en privacy-assuranceopdrachten

Versie 3.0

Juli 2025

#### 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 een bijdrage aan deze versie van de handreiking geleverd:

Jeroen Caron RE MSc CIPP/E, drs. Henk Hendriks RE CISA, drs. Frits Heijman RE RA, drs. Ed Ridderbeekx RE CISA CIPP/E, mr. drs. Jan Roodnat RE RA, mr. Wouter Bas van der Vegt RE CISSP CIPP/E.

#### Coördinatie en redactie versie 3.0: drs. Ed Ridderbeekx RE CISA CIPP/E

**©2018, 2019, 2025 NOREA**, alle rechten voorbehouden

Postbus 242

2130 AE Hoofddorp

telefoon: 088-4960380

e-mail: norea@norea.nl [www.norea.nl](http://www.norea.nl/)

|  |  |
| --- | --- |
| Versiebeheer |  |
| **Versie** | **Datum** | **Wijzigingen** |
| 1.0 | mei 2018 | Eerste versie |
| 2.0 | juni 2019 | Zie paragraaf 10 in Deel 1 van versie 2  |
| 3.0  | juli 2025 | Zie paragraaf 11 in Deel 1 van dit document |

**Inhoudsopgave**

[Deel 1 - Introductie 4](#_Toc203658829)

[1. Inleiding 5](#_Toc203658830)

[2. Doelstellingen van het Privacy Control Framework 5](#_Toc203658831)

[3. Opbouw van het Privacy Control Framework 5](#_Toc203658832)

[4. Het Privacy Control Framework en de AVG 6](#_Toc203658833)

[5. Gebruik van het Privacy Control Framework 6](#_Toc203658834)

[6. PCF en andere privacy-instrumenten van NOREA 8](#_Toc203658835)

[7. PCF en de International Digital Reporting Standards 9](#_Toc203658836)

[8. PCF en certificering volgens de AVG 9](#_Toc203658837)

[9. PCF en ISO 27001/ISO 27002 9](#_Toc203658838)

[10. Totstandkoming van het Privacy Control Framework 10](#_Toc203658839)

[11. Wijzigingen in versie 3.0 10](#_Toc203658840)

[12. Disclaimer 11](#_Toc203658841)

[Deel 2. Onderwerpen en beheersingsdoelstellingen 12](#_Toc203658842)

[Deel 3. Beheersingsmaatregelen 16](#_Toc203658843)

[Deel 4. Capita Selecta 50](#_Toc203658844)

[Bijlage 1. Relatie PCF - AVG 60](#_Toc203658845)

[Bijlage 2. Informatielevenscyclus 66](#_Toc203658846)

[Bijlage 3. PCF en ISO-standaarden 70](#_Toc203658847)

# Deel 1 - Introductie

## Inleiding

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

## 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. De handreiking bevat een verzameling beheersingsdoelstellingen en voorbeelden van maatregelen die gezamenlijk als toetsingscriteria kunnen dienen bij 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 bestaande maatregelen dienen te worden aangevuld of aangepast om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG).

## 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]](#footnote-2)
2. NIST SP800-R53 Privacy Control Catalog;[[2]](#footnote-3)
3. NOREA Raamwerk Privacy Audit;[[3]](#footnote-4)
4. EuroPriSe raamwerk.[[4]](#footnote-5)

In bijlage 2 wordt deze 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 (29 in totaal). Elk privacyonderwerp is gekoppeld aan een beheersingsdoelstelling en deze is vervolgens vertaald naar een aantal beheersingsmaatregelen (72 in totaal) die geëvalueerd kunnen worden. Deel 2 van deze Handreiking biedt een overzicht van de privacyonderwerpen en de hieraan gerelateerde beheersingsdoelstellingen. Deel 3 bevat een gedetailleerde opsomming van illustratieve beheersingsmaatregelen per onderwerp. In paragraaf 5 van deze inleiding wordt nader ingegaan op de betekenis van ‘illustratief’ in dit kader.

## 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 professionele inschatting en op publicaties van de Autoriteit Persoonsgegevens.

Met de implementatie en uitvoering van de maatregelen kan 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 in de context van wettelijke compliance (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.

## 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 PCF-gebruikers onderscheiden:

* 1. De IT-auditor die (1) de privacymaatregelen van een entiteit en het behalen van privacydoelstellingen beoordeelt, met als doel de mate van privacybescherming en/of compliance met wet en regelgeving vast te stellen, of (2) daarover adviseert;
	2. De IT-auditor die een privacy-assuranceopdracht uitvoert op basis van NOREA Richtlijn 3000. Daarnaast is het PCF uitgangspunt als de assuranceopdracht wordt uitgevoerd in het kader van het verkrijgen van een Privacy Audit Proof™ logo.
	3. 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, of die ondersteuning zoeken bij het treffen van privacymaatregelen om aan beheerdoelstellingen te voldoen.

Uitgangspunt is dat de scope van elk van de werkzaamheden zoals hierboven genoemd helder vermeldt tot welke specifieke en risicogebaseerde (verzameling van) verwerking(en) van persoonsgegevens door de entiteit de beoordeling of opdracht zich uitstrekt.

Net als de AVG maakt het PCF onderscheid tussen de rollen van verwerkingsverantwoordelijke en verwerker en de betekenis van die termen is geheel analoog aan de AVG.

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 betrokken professional 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 (illustratieve) beheersingsmaatregelen uit deel 3 dienen te worden beoordeeld, en deze waar nodig te wijzigen, aan te scherpen of aan te vullen naar de context van de betreffende entiteit en 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™-logo. 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 bij assuranceopdrachten *alle* onderwerpen en beheersingsdoelstellingen in deel 2 als uitgangspunt nemen en deze gebruiken als beheersingsraamwerk in het rapport. De 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 illustratief; het is de verantwoordelijkheid van de entiteit om ze, waar nodig, aan de hand van de specifieke kenmerken van de entiteit aan te scherpen, te wijzigen of aan te vullen. 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.

## 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 Data Protection Impact Assessment*

Deze handreiking voor het uitvoeren van impact assessments van de verwerking van persoonsgegevens (PIA of DPIA, AVG: ‘gegevensbeschermingseffectbeoordelingen’) is in 2020 aan een revisie onderworpen om geheel in lijn te worden gebracht met de AVG. De huidige versie 2.0 bestaat uit twee delen, te weten de Handreiking zelf en het ‘NOREA Data Protection Impact Assessment Raamwerk’ met concreet te beantwoorden vragen gedurende de DPIA. 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*

In NOREA’s ‘Handreiking voor SOC 2 en SOC 3 op basis van ISAE3000 / Richtlijn 3000A’ wordt beschreven hoe de privacycategorie opgenomen kan worden in een ISAE 3000/System and Organization Control 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 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’ behorend bij de Trust Services Criteria ten aanzien van privacy.

* *Logo Privacy Audit Proof™*

Op basis van een assurance opdracht die heeft geresulteerd in een goedkeurend oordeel van een privacy-auditor kan aan een entiteit toestemming worden verleend het logo 'Privacy-Audit-Proof' te gebruiken. Het PCF als onderliggend toetsingskader is hierbij uitgangspunt. Voor het nader informatie over het logo en de gebruiksvoorwaarden verwijzen we kortheidshalve naar de website van NOREA.

## PCF en de International Digital Reporting Standards

NOREA heeft een verslaggevingsstandaard ontwikkeld waarmee organisaties zich kunnen verantwoorden over de beheersing van hun informatietechnologie. Dit zijn de *International Digital Reporting Standards* (IDRS; voorheen het NOREA Rapportage Initiatief (NRI)). Privacy is binnen IDRS één van de relevante onderwerpen die een organisatie in overweging moet nemen om verantwoording over af te leggen (naast digitale innovatie en transformatie, data governance en ethiek, outsourcing, cybersecurity en IT continuïteitsmanagement).

IDRS bevat vereiste *disclosures* in de verslaggeving over privacy, alsmede handreikingen (*guidance)* om hieraan invulling te geven. Alhoewel er thematisch sterke raakvlakken zijn tussen het privacy-onderdeel van IDRS enerzijds en het PCF anderzijds, dienen zij uiteraard een ander doel. Wel zal het IDRS worden aangevuld met een audithandreiking, waarmee onafhankelijke IT-auditors assurance kunnen geven over de getrouwe weergave van de IT-verantwoording (conform IDRS) door een organisatie.

## PCF en certificering volgens de AVG

De AVG zelf onderstreept het belang van certificeringsmechanismen om compliance met de AVG aan te tonen. Het PCF mag niet worden gezien als een verzameling criteria die een certificering zoals bedoeld in artikelen 42 en 43 van de AVG mogelijk maakt, alhoewel het het in beginsel voldoet aan de richtlijnen die de European Data Protection Board (EDPB) over AVG-certificering heeft uitgebracht.

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).

Op het moment van opstellen van dit PCF is het in Nederland nog niet mogelijk een formeel privacycertificaat te verkrijgen zoals bedoeld in de artikelen 42 en 43 van de AVG. Wel is het mogelijk om op basis van het onderzoek door een onafhankelijke 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.

## 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 zekere overlap tussen het PCF en normenkaders die zich richten op informatiebeveiliging in zijn algemeenheid. Een voorbeeld van dit laatste zijn ISO/IEC ISO 27001 en 27002, die dienen als een standaard 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 Overheid (BIO)), hebben hun wortels in ISO 27001/27002. In bijlage 3 van dit document wordt ingegaan op een aantal aspecten van de relatie tussen het PCF en ISO 27001/27002, alsmede op het verband tussen het PCF en de privacygerelateerde ISO standaarden 27701, 27018 en 29100.

## Totstandkoming van het Privacy Control Framework

De eerste versie van het PCF is tussen november 2017 en april 2018 opgesteld door een werkgroep van NOREA. Versie 1.0 werd uitgebracht in mei 2018 na goedkeuring door de Vaktechnische Commissie van NOREA.

In mei/juni 2019 is een update van het PCF (versie 2.0) gemaakt, dat is getoetst door een klankbordgroep van leden van de Kennisgroep Privacy van NOREA, is voorgelegd aan de Vaktechnische Commissie en in augustus 2019 is gepubliceerd.

Eind 2024 is opnieuw een revisie van het PCF gestart onder regie van de Kennisgroep Privacy van NOREA. Die revisie heeft geleid tot vaststelling en publicatie van de voorliggende versie 3.0, wederom na goedkeuring door de Vaktechnische Commissie en het bestuur van NOREA.

## Wijzigingen in versie 3.0

In de update van versie 2.0 naar versie 3.0 van het PCF zijn de volgende wijzigingen doorgevoerd:

* tekstuele correctie, verduidelijking, en aanscherpingen van alle delen;
* revisie en actualisering van de inleidende paragrafen (deel 1);
* revisie en waar nodig herformulering van de beheersingsdoelstellingen per onderwerp (deel 2).
* revisie en waar nodig herformulering van de beheersingsmaatregelen per onderwerp (deel 3).
* revisie en actualisering van de bijlagen 1 en 3, waarbij met name bijlage 3 is aangepast op basis van de 2022-versie van ISO 27001;
* toevoeging capita selecta (deel 4);
* rationalisatie van het onderwerp ‘Gegevensbeveiliging’ in deel 3 (zie aldaar voor een nadere toelichting);
* samenvoeging van de onderdelen met betrekking tot rechten van betrokkenen (DAR, DCR, DDR, en DPR) tot één onderdeel (DSR);
* een duidelijker onderscheid tussen de taken en verantwoordelijkheden van een Privacy Officer en die van de Functionaris Gegevensbescherming (FG). Waar het PCF nu spreekt over een FG wordt gedoeld op de in de AVG (art. 37 t/m 39) omschreven functie.

Door deze wijzigingen omvat PCF 3.0 72 beheersingsmaatregelen, 24 minder dan in PCF 2.0.

## Disclaimer

Het PCF is ontwikkeld om IT-auditors en entiteiten te ondersteunen bij de beoordeling van het stelsel van maatregelen voor privacybeheersing. Ondanks NOREA’s inspanningen om een omvattend en praktisch bruikbaar raamwerk samen te stellen blijft toepassing van het PCF de verantwoordelijkheid van de gebruiker. Het PCF biedt geen juridisch advies, certificering of garanties met betrekking tot AVG-compliance.

# Deel 2. Onderwerpen en beheersingsdoelstellingen

De onderstaande tabel geeft een overzicht van het Privacy Control Framework. Het raamwerk bevat in totaal 72 beheersingsmaatregelen, verdeeld over 29 onderwerpen in 9 fasen van levenscyclusmanagement. In deel 3 worden de beheersingsmaatregelen per onderwerp/beheersingsdoelstelling weergegeven.

| **Fase levenscyclus** | **Topic** | **Onderwerp** | **Beheersingsdoelstelling** | **# Beheersings-maatregelen** |
| --- | --- | --- | --- | --- |
| **Management** | PPO | Privacybeleid | De wijze waarop de entiteit persoonsgegevens verwerkt is verankerd in een beleidskader dat rekening houdt met geaccepteerde privacyprincipes en van toepassing zijnde wet- en regelgeving. | 5 |
| RRE | Afbakening van rollen en verantwoordelijkheden | Rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacydoelstellingen zijn duidelijk gedefinieerd en belegd. | 5 |
| PDI | Identificatie en classificatie van persoonsgegevens | De entiteit heeft een volledig en gedocumenteerd overzicht van de verwerkingen van persoonsgege-vens en de karakteristieken van de verwerkingen. De entiteit houdt hierbij rekening met verschillen in de gevoeligheid van persoonsgegevens. | 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 |
| PIA | Data protection impact assessments | De privacy-gerelateerde effecten van nieuwe producten en diensten, of van wijzigingen op bestaande producten en diensten worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt. | 5 |
| PIB | Beheer van privacyincidentenen inbreuken | De entiteit detecteert incidenten met betrekking tot privacy en beperkt de gevolgen daarvan op adequate wijze. De entiteit neemt maatregelen om toekomstige inbreuken te voorkomen. | 8 |
| SCO | Competenties medewerkers | Medewerkers die vanwege hun functie met persoonsgegevens omgaan hebben de noodzakelijke competenties om dat zorgvuldig te doen. | 3 |
| SAT | Bewustwording en training medewerkers | Medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacybeleid en de -richtlijnen binnen de entiteit, en hun verantwoordelijkheden met betrekking tot privacy. | 3 |
| LRC | Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten | Privacybeheersing binnen de entiteit is in overeenstemming met bedrijfsvereisten (structuur, strategie, (keten)samenwerking) en wet- en regelgeving. | 1 |
| **Informeren** | PST | Privacyverklaring | De entiteit is naar betrokkenen transparant over haar privacybeheersing.  | 2 |
| **Keuze en toestemming** | CFR | Toestemmingsraamwerk | De entiteit heeft waar vereist of noodzakelijk toestemming van betrokkenen verkregen om persoonsgegevens te verwerken. | 4 |
| **Verzamelen** | DMI | Minimale gegevensverwerking | De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. | 2 |
| **Gebruiken, opslaan en verwijderen** | ULI | Doelbinding | Persoonsgegevens worden uitsluitend verstrekt, beschikbaar gesteld of anderszins verwerkt voor de doeleinden die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij afwij-kingen daarvan wettelijk vereist zijn of de betrokkene daartoe toestemming heeft gegeven. | 2 |
| PBD | Gegevens-bescherming door ontwerpen door standaard-instellingen) | De entiteit neemt privacymaatregelen op een pro-actieve, doelmatige en doeltreffende manier en neemt bij het ontwikkelen en wijzigen van producten, diensten, systemen of processen het privacy-beleid, solide 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 | De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschik-baar nadat de bewaartermijn is verstreken. | 2 |
| URE | Gebruik en beperking | Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft bepaald of wanneer er sprake is van specifieke juridische restricties. | 2 |
| **Inzage en kwaliteit van gegevens** | DSR | Verzoeken van betrokkenen | Verzoeken van betrokkenen met betrekking tot inzage, correcties, verwijdering, en overdracht van hun persoonsgegevens worden op een juiste en tijdige wijze afgehandeld. | 3 |
| ACD | Juistheid en volledigheid van gegevens | De entiteit heeft een proces om de juistheid en volledigheid van verwerkte persoonsgegevens te waarborgen. | 2 |
| **Verstrekken** | TPD | Verstrekking aan derden en registratie | Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis. | 1 |
| TPA | Overeenkomstenmet derden | Inschakeling van diensten (gerelateerd aan persoonsgegevens) van derden doet geen afbreuk aan het niveau van privacybeheersing van de entiteit. | 3 |
| DTR | Doorgifte van persoonsgegevens | Persoonsgegevens worden niet doorgegeven aan entiteiten in landen wier rechtskader ontoereikende waarborgen biedt ten aanzien van de privacy van betrokkenen. | 2 |
| **Gegevens-beveiliging** | ISP | Programma informatiebeveiliging | Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, kwaadwillige handelingen zoals hacken, diefstal of ongeautoriseerde verstrekking. | Niet gespecificeerd[[5]](#footnote-6) |
| 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. | Niet gespecificeerd |
| STR | Veilige gegevensoverdracht | Tijdens verzending of overdracht worden persoonsgevens beschermd tegen ongeautoriseerde toegang of kennisname. | Niet gespecificeerd |
| ENC | Versleuteling en eindpuntbeveiliging | De vertrouwelijkheid van persoonsgegevens wordt gewaarborgd en inbreuken op persoonsgegevens of verlies van media leiden niet automatisch tot ongeautoriseerde inzage. | Niet gespecificeerd |
| LOG | Registreren van toegang | De entiteit registreert en onderzoekt toegang of toegangspogingen tot persoonsgegevens door medewerkers, derden of hackers die zouden kunnen duiden op of leiden tot ongeautoriseerde in-breuken op persoonsgegevens. | Niet gespecificeerd |
| **Monitoren en handhaven** | REV | Beoordeling van compliance met privacywetgeving | De entiteit heeft een proces waarbij compliance met wet- en regelgeving met betrekking tot privacy bij voortduring wordt getoetst. | 1 |
|  | MON | Periodiek monitoren van privacybeheersings-maatregelen | De entiteit toetst periodiek of getroffen beheersmaatregelen effectief zijn in relatie tot de privacyrisico’s van de entiteit. | 3 |

# Deel 3. Beheersingsmaatregelen

[Management 19](#_Toc203657717)

[Informeren 31](#_Toc203657718)

[Keuze en toestemming 33](#_Toc203657719)

[Verzamelen 35](#_Toc203657720)

[Gebruiken, opslaan en verwijderen 36](#_Toc203657721)

[Inzage en kwaliteit van gegevens 41](#_Toc203657722)

[Verstrekken 43](#_Toc203657723)

[Gegevensbeveiliging 46](#_Toc203657724)

De volgende pagina’s geven een opsomming van de beheersingsmaatregelen van het PCF, geordend per onderwerp en per fase uit het levenscyclusmodel (zie bijlage 2). Voor elk onderwerp wordt de beheersingsdoelstelling 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 wijze waarop de entiteit persoonsgegevens verwerkt is verankerd in een beleidskader dat rekening houdt met geaccepteerde privacyprincipes en 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 andere belanghebbenden. Het privacybeleid wordt jaarlijks door het management geëvalueerd en (opnieuw) vastgesteld. | VV, V |
| PPO02 | Het management brengt zijn commitment aan (en verantwoordelijkheid voor) gegevensverwerking in lijn met 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 algemeen geaccepteerde privacyprincipes en wettelijke voorschriften 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 (verwerkingsverantwoordelijken) vastgelegd zijn. | VVV |
| PPO05 | De entiteit heeft een onderbouwde vastlegging van de rechtmatigheid en grondslag van elke verwerking van persoonsgegevens. | VV |
| *Gerelateerde kernelementen van de AVG:** Privacyprincipes
* Rechtmatigheid van de verwerking
* Register van de verwerkingsactiviteiten
 |

|  |
| --- |
| **Afbakening van rollen en verantwoordelijkheden (RRE)***Beheersingsdoelstelling:*Rollen en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en het behalen van privacydoelstellingen zijn duidelijk gedefinieerd en belegd.  |
| *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 en bescherming van persoonsgegevens 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 de 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 op basis van ‘overerving’ van verplichtingen. | VVV |
| RRE04 | De entiteit belast een of meerdere personen met de verantwoordelijkheid voor (de coördinatie van ) de privacybeheersing[[6]](#footnote-7). De taken bevoegdheden en verantwoordelijkheden van deze perso(o)n(en) 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 aan die medewerkers gecommuniceerd. | VV, V |
| RRE06 | Indien vereist door wet- en regelgeving wijst de organisatie een Functionaris Gegevensbescherming (FG) aan en belast die met advies over en toezicht op de verwerking van persoonsgegevens, in overeenstemming met de eisen die de wet aan de functie van FG stelt. | 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 volledig en gedocumenteerd overzicht van de verwerkingen van persoonsgegevens en de karakteristieken van de verwerkingen. De entiteit houdt hierbij rekening met verschillen in de gevoeligheid van persoonsgegevens.  |
| *Fase informatielevenscyclusmanagement:* **Management** |
| *Beheersingsmaatregelen:* |  |
| PDI01 | De entiteit identificeert en documenteert verwerking van persoonsgegevens aan de hand van een gedocumenteerd proces, en classificeert persoonsgegevens 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 documenteert en beoordeelt de rechtmatigheid van de (geplande) verwerkingen uitvoerig en treft maatregelen 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, doorgiften, en waar mogelijk beveiligingsmaatregelen). De juistheid en volledigheid van dit register wordt jaarlijks beoordeeld. (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). De juistheid en volledigheid van dit register wordt jaarlijks beoordeeld. | VVV |
| *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:1. gebeurtenissen en factoren te identificeren die het behalen van de privacydoelstellingen in gevaar brengen;
2. 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 (sinds v2.0).* |  |
| RMA03 | Wanneer nieuwe of gewijzigde privacyrisico's worden gesignaleerd, worden de privacyrisicobeoordeling en de risicobeheerstrategieën herzien en zo nodig bijgewerkt. | VV, V |
| RMA04 | Het management heeft acceptatiecriteria voor privacyrisico’s vastgesteld, goedgekeurd, gedocumenteerd en past deze toe. | VV, V |
| RMA05 | De entiteit implementeert de beheersingsmaatregelen zoals bedoeld in RMA01(b) en beoordeelt de effectiviteit van hun implementatie.  | 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, of van wijzigingen op bestaande producten en diensten 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 eventueel voorafgegaan door een pre-DPIA).  | VV |
| PIA02 | Bij de DPIA wordt vastgesteld:1. de aard van de geplande verwerkingen;
2. hun doelstelling, noodzaak, en proportionaliteit;
3. de risico's die beoogde verwerkingen met zich meebrengen voor rechten en vrijheden van betrokkenen;
4. welke maatregelen moeten worden genomen om deze risico's te beperken.
 | VV |
| ~~PIA03~~ | *Samengevoegd met PIA02 (sinds v2.0)*. |  |
| 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 gepland en worden doorgevoerd. | VV |
| PIA06 | Een verandermanagementproces is vastgesteld om ervoor zorg te dragen dat de in de DPIA vastgestelde privacymaatregelen in de beoogde nieuwe of gewijzigde processen/producten/diensten worden geïmplementeerd. DPIA’s worden periodiek herhaald. | VV |
| *Gerelateerde kernelementen van de AVG:** Gegevensbeschermingseffectbeoordeling
 |

Zie ook**:**

*NOREA Handreiking Data Protection Impact Assessment, versie 2.0, juli 2020*

*Bijlage 4, Capita Selecta: Data localisation, internationale datatransfers, en DTIA’s*

|  |
| --- |
| **Beheer van privacyincidenten en inbreuken (PIB)***Beheersingsdoelstelling:*De entiteit detecteert incidenten met betrekking tot privacy en beperkt de gevolgen daarvan op adequate wijze. De entiteit neemt maatregelen om toekomstige inbreuken te voorkomen. |
| *Fase informatielevenscyclusmanagement:* **Management** |
| *Beheersingsmaatregelen:* |  |
| PIB01 | De entiteit heeft een formeel proces vastgesteld en geïmplementeerd dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens, waarin het volgende is vastgelegd:1. 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;
2. De privacy officer (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 privacy officer of FG de aard van de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens(verzamelingen) en betrokkenen in kwestie.
3. De privacy officer initieert en coördineert de nodige correctieve 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).
4. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en licht het management in (en, indien van toepassing, de verwerkingsverantwoordelijke en de toezichthouder).
 | VV, V |
| ~~PIB02~~ | *Samengevoegd met PIB06 (sinds v2.0)* |  |
| 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 ingelicht wanneer het waarschijnlijk is dat een inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. (b) De entiteit heeft een beleid ten aanzien van het melden van een inbreuk op de beveiliging. Dit is gericht op tijdige inlichting van de betreffende verwerkingsverantwoordelijke over een dergelijke (mogelijke) inbreuk. | VVV |
| 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. | VVV |
| PIB06 | De aangewezen privacy officer 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 | De procedure voor beheer van privacyincidenten en -inbreuken waarborgt dat op basis van de lering die uit de inbreuk wordt getrokken correcties en verbeteringen worden doorgevoerd, en dat de ‘lessons learned’ worden gebruikt in bewustwordingsprogramma's voor medewerkers. | VV, V |
| PIB08 | De procedure voor beheer van privacyincidenten en -inbreuken waarborgt dat:1. na elk beveiligingsincident en inbreuk met betrekking tot persoonsgegevens ('datalekken') en elke grootschalige inbreuk in verband met persoonsgegevens een formele incidentbeoordeling wordt uitgevoerd, waarbij indien nodig externe expertise wordt ingeschakeld;
2. incidenten worden geëvalueerd en de noodzakelijke verbeteringen worden geïdentificeerd op basis van:
	* de onderliggende oorzaak van het incident;
	* incidentpatronen;
	* wijzigingen in de interne controle en wetgeving;
3. De resultaten van de 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 geëvealueerd en zonodig herzien, en tevens (1) kort na de implementatie van ingrijpende wijzigingen in systemen of procedures, en (2) nadat zich een ernstig incident heeft voorgedaan. | VV, V |
| *Gerelateerde kernelementen van de AVG:** Inbreuk in verband met persoonsgegevens
 |

|  |
| --- |
| **Competenties medewerkers (SCO)***Beheersingsdoelstelling:*Medewerkers die vanwege hun functie met persoonsgegevens omgaan hebben de noodzakelijke competenties om dat zorgvuldig te doen. |
| *Fase informatielevenscyclusmanagement:* **Management** |
| *Beheersingsmaatregelen:* |  |
| SCO01 | De entiteit heeft de competenties gedocumenteerd van privacy medewerkers die met persoonsgegevens werken. De entiteit legt daarnaast vast hoe deze competenties kunnen worden verworven (o.a. door trainingen). | VV, V |
| SCO02 | De entiteit documenteert in hoeverre individuele medewerkers die met persoonsgegevens werken over deze competenties beschikken en heeft een procedure opgesteld om lacunes in competenties en vaardigheden aan te vullen. | VV, V |
| SCO03 | De entiteit besteedt bij de werving en onboarding van nieuwe medewerkers die zullen werken met persoonsgegevens aandacht aan competenties met betrekking tot privacy. De omgang met persoonsgegevens is een van de punten in individuele beoordelingsgesprekken. | VV, V |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
* Privacyprincipes
* Functionaris voor gegevensbescherming
 |

|  |
| --- |
| **Bewustwording en training medewerkers (SAT)***Beheersingsdoelstelling:*Medewerkers zijn voldoende op de hoogte van de privacywetgeving en -regelgeving, het privacybeleid en de -richtlijnen binnen de entiteitorganisatie, en hun verantwoordelijkheden met betrekking tot privacy.  |
| *Fase informatielevenscyclusmanagement:* **Management** |
| *Beheersingsmaatregelen:* | *Bevindingen/toetsing:* |
| SAT01 | Ten minste eenmaal per jaar wordt voor alle medewerkers een bewustwordingstraining ten aanzien van privacy en beveiliging georganiseerd. Nieuwe medewerkers, contractanten en anderen wordt verplicht om binnen een redelijke termijn na aanvang van hun overeenkomst met de entiteit 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.  | VV, V |
| SAT03 | Trainingen en bewustwordingscursussen worden jaarlijks geëvalueerd en geactualiseerd (bijvoorbeeld op basis van incidenten die zich hebben voorgedaan) 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
 |

|  |
| --- |
| **Beoordeling van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten (LRC)***Beheersingsdoelstelling:*Privacybeheersing binnen de entiteit is in overeenstemming met bedrijfsvereisten (structuur, strategie, (keten)samenwerking) en wet- en regelgeving. |
| *Fase informatielevenscyclusmanagement:* **Management** |
| *Beheersingsmaatregelen:* |  |
| LRC01 | De entiteit heeft een proces ingericht waarin de implicaties op privacybeleid en -beheersingsmaatregelen worden vastgesteld, beoordeeld en behandeld van wijzigingen in:1. wet- en regelgeving;
2. sectorspecifieke eisen, best practices en richtlijnen;
3. 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);
4. bedrijfsactiviteiten en processen;
5. personen die worden belast met de verantwoordelijkheid voor privacy en beveiliging;
6. technologie (voordat deze wordt geïmplementeerd).
 | VV, V |
| *Gerelateerde kernelementen van de AVG:** Gegevensbeschermingseffectbeoordeling
* Rechtmatigheid van de verwerking
 |

Informeren

|  |
| --- |
| **Privacyverklaring (PST)***Beheersingsdoelstelling:*De entiteit is naar betrokkenen transparant over haar privacybeheersing.  |
| *Fase informatielevenscyclusmanagement:* **Informeren** |
| *Beheersingsmaatregelen:* |  |
| PST01 | In de privacyverklaring van de entiteit staat:1. welke persoonsgegevens worden verzameld, waar deze informatie vandaan komt, de doeleinden voor de verzameling en de betreffende rechtsgronden voor de verwerking;
2. wat de gevolgen zijn, voor zover daar sprake van is, als de betrokkene de gevraagde gegevens niet verstrekt;
3. informatie over verdere verwerking (indien van toepassing);
4. informatie over de rechten van betrokkenen en de wijze waarop zij die rechten kunnen uitoefenen (zie ook URE, DSR);
5. contact gegevens van de entiteit en -indien van toepassing- de FG.
 | VV |
| PST02 | De privacyverklaring:1. is gemakkelijk toegankelijk en beschikbaar voor betrokkenen op het moment dat voor het eerst persoonsgegevens van de betrokkene worden verzameld;
2. 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;
3. 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;
4. is eenvoudig te begrijpen en leesbaar;
5. wordt jaarlijks geëvalueerd en waar nodig bijgesteld.
 | VV |
| *Gerelateerde kernelementen van de AVG:** Rechten van de betrokkene
* Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker
* Privacyprincipes
 |

Keuze en toestemming

|  |
| --- |
| **Toestemmingsraamwerk (CFR)***Beheersingsdoelstelling:*De entiteit heeft waar vereist of noodzakelijk toestemming van betrokkenen verkregen om persoonsgegevens te verwerken. |
| *Fase informatielevenscyclusmanagement:* **Keuze en toestemming** |
| *Beheersingsmaatregelen:* | *Bevindingen/toetsing:* |
| CFR01 | In de privacyverklaring beschrijft de entiteit op duidelijke en beknopte wijze:1. welke keuzes de betrokkene heeft met betrekking tot de verzameling, het gebruik, en de verstrekking van persoonsgegevens;
2. 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);
3. de mogelijkheid om de contactvoorkeuren aan te passen en hoe de betrokkene dit doet;
4. wat de gevolgen zijn als de persoonsgegevens die nodig zijn voor een transactie of dienst niet worden verstrekt;
5. 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:1. 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);
2. legt de entiteit de voorkeuren van de betrokkene vast (schriftelijk of elektronisch);
3. documenteert de entiteit wijzigingen in de contactvoorkeuren en verwerkt deze;
4. zorgt de entiteit dat de voorkeuren van de betrokkene tijdig worden verwerkt;
5. bewaart de entiteit de informatie om aan kunnen te tonen dat de betrokkene toestemming heeft verleend.
 | VV |
| CFR03 | De entiteit verzamelt of verwerkt geen bijzondere categorieën van persoonsgegevens, tenzij daar een duidelijke wettelijke basis voor geldt. De entiteit documenteert in dat geval deze basis.  | 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 doeleinden waarvoor zij worden verwerkt. |
| *Fase informatielevenscyclusmanagement:* **Verzamelen** |
| *Beheersingsmaatregelen:* |  |
| DMI01 | De entiteit richt een proces en procedures in om:1. te bepalen welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking;
2. de verwerking van persoonsgegevens te beperken tot het voor het doel noodzakelijke minimum;
3. jaarlijks 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 de entiteit minimale gegevensverwerking als een privacyprincipe hanteert (zie PPO). | VV |
| *Gerelateerde kernelementen van de AVG:** Privacyprincipes
* Gegevensbescherming door ontwerp / door standaardinstellingen
 |

Gebruiken, opslaan en verwijderen

|  |
| --- |
| **Doelbinding (ULI)***Beheersingsdoelstelling:*Persoonsgegevens worden uitsluitend verstrekt, beschikbaar gesteld of anderszins verwerkt voor de doeleinden die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij afwijkingen daarvan wettelijk vereist zijn of de betrokkene daartoe toestemming heeft gegeven. |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** |
| *Beheersingsmaatregelen:* |  |
| ULI01 | De entiteit heeft een proces en procedures ingericht om:1. de verstrekking en het gebruik van persoonsgegevens te beperken tot de doeleinden die worden genoemd in het privacybeleid en de privacyverklaring van de entiteit;
2. als de wettelijke grondslag ‘toestemming’ is, 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 de entiteit doelbinding als een privacyprincipe hanteert (zie PPO). | VV |
| *Gerelateerde kernelementen van de AVG:** Privacyprincipes
* Gegevensbescherming door ontwerp / door standaardinstellingen
 |

|  |
| --- |
| **Gegevensbescherming door ontwerp en door standaardinstellingen (PBD)***Beheersingsdoelstelling:*De entiteit neemt privacymaatregelen op een pro-actieve, doelmatige en doeltreffende manier en neemt bij het ontwikkelen en wijzigen van producten, diensten, systemen of processen het privacy-beleid, solide privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht. |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** |
| *Beheersingsmaatregelen:* |  |
| PBD01 | Bij de (besluitvorming over) ontwikkeling, het ontwerp, en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, brengt de entiteit zo vroeg mogelijk in het ontwerpproces privacyrisico’s in kaart en adresseert deze (in relatie tot de rechten en vrijheden van betrokkenen en het privacybeleid van de entiteit).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, gedocumenteerd en geïmplementeerd onderdeel van de projectmethodiek en/of het (product)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 privacyvriendelijke opties met betrekking tot privacy. | VV |
| *Gerelateerde kernelementen van de AVG:** Gegevensbescherming door ontwerp / door standaardinstellingen
* Privacyprincipes
 |

Zie ook**:**

*Bijlage 4, Capita Selecta:* Privacy by Design

|  |
| --- |
| **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:1. documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens;
2. bewaart persoonsgegevens niet langer dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of wettelijke verplichting;
3. documenteert voor elke verwerking van persoonsgegevens de betreffende bewaartermijn;
4. informeert betrokkenen in de privacyverklaring over (het beleid ten aanzien van) bewaartermijnen;
5. slaat gearchiveerde kopieën en back-ups op, bewaart en verwijdert deze overeenkomstig het bewaarbeleid;
6. instrueert verwerkers over bewaartermijnen.
 | VV |
| DRE02 | Bij het vaststellen van bewaarprocedures worden wettelijke en contractuele bewaartermijnen in acht genomen. | VV |
| *Gerelateerde kernelementen van de AVG:** Privacyprincipes
* Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker
 |

|  |
| --- |
| **Verwijdering, vernietiging en anonimisatie (DDA)***Beheersingsdoelstelling:*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 en geïmplementeerd om te waarborgen dat:1. het wissen en vernietigen van persoonsgegevens geschiedt conform het beleid van de entiteit, ongeacht de vorm waarin deze zijn opgeslagen (zoals elektronisch, op optische media, of op papier);
2. de verwijdering van originele, gearchiveerde gegevens, back-ups en persoonlijke kopieën conform het vernietigingsbeleid plaatsvindt;
3. de verwijdering van persoonsgegevens op een adequate wijze wordt vastgelegd.

De entiteit zorgt er daarnaast voor dat:1. persoonsgegevens worden gelokaliseerd en verwijderd of overgedragen, voor zover dit technisch mogelijk is.
2. 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 systematische basis worden vernietigd, gewist of geanonimiseerd.
 | VV |
| DDA02 | Bij het vaststellen van procedures voor verwijdering, vernietiging en vermindering van persoonsgegevens worden contractbepalingen in acht genomen. | VV |
| *Gerelateerde kernelementen van de AVG:** Privacyprincipes
* Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker
* Beveiliging van de verwerking
* Gegevensbescherming door ontwerp / door standaardinstellingen
 |

Zie ook**:**

*Bijlage 4, Capita Selecta:* Anonimisatie

|  |
| --- |
| **Gebruik en beperking (URE)***Beheersingsdoelstelling:*Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft bepaald of wanneer er sprake is van specifieke juridische restricties.  |
| *Fase informatielevenscyclusmanagement:* **Gebruiken, opslaan en verwijderen** |
| *Beheersingsmaatregelen:* |  |
| ~~URE01~~ | *Samengevoegd met PST01 (sinds v2.0).* |  |
| 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, voorzover van toepassing, 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

|  |
| --- |
| **Verzoeken van betrokkenen (DSR)***Beheersingsdoelstelling:*Verzoeken van betrokkenen met betrekking tot inzage, correcties, verwijdering, en overdracht van hun persoonsgegevens worden op een juiste en tijdige wijze afgehandeld.  |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** |
| *Beheersingsmaatregelen:* |  |
| DSR01 | De entiteit heeft procedures ingericht en past deze toe om adequaat te reageren op verzoeken van betrokkenen met betrekking tot hun persoonsgegevens. Deze procedures gaan in ieder geval in op verzoeken tot (1) inzage, (2) correcties, (3) verwijdering, en (4) overdracht van persoonsgegvens.  | VV |
| DSR02 | De entiteit verifieert de identiteit van de betrokkene alvorens diens verzoek om inzage, correcties, verwijdering, of overdracht te honoreren.  | VV |
| DSR03 | De entiteit registreert verzoeken van betrokkenen en de wijze waarop deze zijn afgehandeld. | VV |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
* Gegevensbescherming door ontwerp / door standaardinstellingen
* Rechten van de betrokkene
 |

|  |
| --- |
| **Juistheid en volledigheid van gegevens (ACD)***Beheersingsdoelstelling:*De entiteit heeft een proces om de juistheid en volledigheid van verwerkte persoonsgegevens te waarborgen. |
| *Fase informatielevenscyclusmanagement:* **Inzage en kwaliteit van gegevens** |
| *Beheersingsmaatregelen:* |  |
| ACD01 | De entiteit heeft procedures opgesteld en geïmplementeerd om:1. persoonsgegevens aan te passen en te valideren wanneer deze worden verzameld, gecreëerd, bijgehouden en bijgewerkt;
2. de datum vast te leggen waarop de persoonsgegevens zijn verkregen of bijgewerkt;
3. te specificeren wanneer de persoonsgegevens niet meer geldig zijn;
4. 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);
5. in redelijkheid de juistheid en volledigheid te verifiëren van persoonsgegevens die zijn verkregen van de betrokkene of van derden, of die zijn verstrekt aan derden;
6. te waarborgen dat de verwerkte persoonsgegevens juist en volledig genoeg zijn om beslissingen op te baseren.
 | VV |
| ACD02 | De entiteit voert jaarlijks 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. |
| *Fase informatielevenscyclusmanagement:* **Verstrekken** |
| *Beheersingsmaatregelen:* |  |
| TPD01 | De entiteit heeft procedures ingericht om:1. te voorkomen dat persoonsgegevens aan derden worden verstrekt, tenzij daarvoor een wettelijke basis bestaat;
2. te documenteren wat de aard van de persoonsgegevens is die aan derden worden verstrekt en in welke mate deze worden verstrekt;
3. 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;
4. te documenteren of persoonsgegevens aan derden worden verstrekt onder een juridische verplichting;
5. 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
 |

Zie ook**:**

*Bijlage 4, Capita Selecta: Data localisation, internationale datatransfers, en DTIA’s*

|  |
| --- |
| **Overeenkomsten met derden (TPA)***Beheersingsdoelstelling:*Inschakeling van diensten (gerelateerd aan persoonsgegevens) van derden doet geen afbreuk aan het niveau van privacybeheersing van de entiteit.  |
| *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. (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. | VVV |
| TPA02 | De entiteit zorgt dat in de overeenkomsten eveneens de volgende verplichtingen voor de andere partij zijn opgenomen:1. vertrouwelijkheids- en geheimhouding;
2. beveiligingsvereisten;
3. medewerking bij het behandelen van verzoeken van betrokkenen en de uitoefening van rechten van de betrokkenen;
4. informatieverstrekking (bijv. in het geval van geplande uitbesteding);
5. informatieverstrekking en medewerking bij inbreuken in verband met persoonsgegevens;
6. bewaartermijnen en verwijdering van gegevens;
7. geen verdere uitbesteding zonder toestemming van de entiteit;
8. auditrechten;
9. aansprakelijkheid en vrijwaring.
 | VV, V |
| TPA03 | De entiteit evalueert periodiek de prestaties en de naleving van de verplichtingen door derden/leveranciers en neemt waar nodig corrigerende acties die uit deze evaluatie voortvloeien.  | 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 aan entiteiten in landen wier rechtskader on-toereikende waarborgen biedt ten aanzien van de privacy van betrokkenen. |
| *Fase informatielevenscyclusmanagement:* **Verstrekken** |
| *Beheersingsmaatregelen:* |  |
| DTR01 | De entiteit heeft alle gevallen in kaart gebracht waarin persoonsgegevens waar zij de verantwoordelijkheid voor draagt (zullen) worden doorgegeven aan en verwerkt in derde landen of door internationale organisaties die mogelijk de privacy van betrokkenen niet voldoende waarborgen. | VV, V |
| DTR02 | De entiteit geeft alleen persoonsgegevens door aan entiteiten in derde landen (a) waarvoor de Europese Commissie een adequaatheidsbesluit heeft genomen, of (b) die een passend beschermingsniveau voor persoonsgegevens bieden (bijv. bindende bedrijfsvoorschriften of standaardbepalingen inzake gegevensbescherming). | VV, V |
| *Gerelateerde kernelementen van de AVG:** Doorgiften van persoonsgegevens aan derde landen of internationale organisaties
 |

Zie ook**:**

*Bijlage 4, Capita Selecta: Data localisation, internationale datatransfers, en DTIA’s*

Gegevensbeveiliging

In tegenstelling tot de andere onderwerpen in dit deel van het PCF, en in afwijking van versie 2.0, is ervoor gekozen bij het onderdeel ‘Gegevensbeveiliging’ geen illustratieve beheersingsmaatregelen op te nemen maar te volstaan met het aangeven van beheersingsdoelstellingen. De redenen hiervoor zijn als volgt.

Bij ‘gegevensbeveiliging’ gaat het in de context van privacy om het gebied waar de te nemen (beveiligings)maatregelen een grote mate van overlap vertonen met organisatorische en technische beveiligingsmaatregelen, die een entiteit al heeft getroffen in het kader van haar (meer algemene) verantwoordelijkheid voor informatiebeveiliging.

Daarbij komt dat deze maatregelen veelal een uitwerking zijn van reeds bestaande normenkaders die binnen entiteiten als referentie of standaardniveau van informatiebeveiliging zijn vastgesteld (denk hierbij aan ISO 27001, BIO, CobIT, NIST). Het op deze plaats benoemen van specifieke informatiebeveiligingsmaatregelen voor privacy (zoals in versie 2.0 van het PCF), ook al zijn die illustratief, brengt dan het risico met zich mee van *cherry-picking* waarbij onvoldoende recht wordt gedaan aan het brede spectrum van beveiligingsmaatregelen die in het kader van privacy relevant kunnen zijn.

Gebruikers van het PCF wordt aangeraden de organisatorische en technische beveiligingsmaatregelen die binnen een entiteit voor privacybeheersing van toepassing zijn zelf te formuleren op basis van binnen die entiteit gehanteerde normen- of referentiekaders, en gebruikmakend van de beheersingsdoelstellingen van het PCF, die we in het onderstaande wél hebben gehandhaafd.

Volledigheidshalve verwijzen we ook naar bijlage 3 van dit document, waarin de relatie van het PCF met een aantal ISO standaarden wordt verduidelijkt.

|  |
| --- |
| **Programma informatiebeveiliging (ISP)***Beheersingsdoelstelling:*Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, kwaadwillige handelingen zoals hacken, diefstal of ongeautoriseerde verstrekking. |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
 |
| **Identiteit en toegangsbeheer (IAM)***Beheersingsdoelstelling:*Toegangsrechten tot persoonsgegevens zijn uitsluitend toegekend aan geautoriseerde personen wier identiteit adequaat wordt geauthenticeerd.  |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
 |

|  |
| --- |
| **Veilige gegevensoverdracht (STR)***Beheersingsdoelstelling:*Tijdens verzending of overdracht worden persoonsgevens beschermd tegen ongeautoriseerde toegang of kennisname.  |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
* Inbreuk in verband met persoonsgegevens
 |

|  |
| --- |
| **Versleuteling en eindpuntbeveiliging (ENC)***Beheersingsdoelstelling:*De vertrouwelijkheid van persoonsgegevens wordt gewaarborgd en inbreuken op persoonsgegevens of verlies van media leiden niet automatisch tot ongeautoriseerde inzage.  |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
* Inbreuk in verband met persoonsgegevens
 |

|  |
| --- |
| **Registreren van toegang (LOG)***Beheersingsdoelstelling:*De entiteit registreert en onderzoekt toegang of toegangspogingen tot persoonsgegevens door medewerkers, derden of hackers die zouden kunnen duiden op of leiden tot ongeautoriseerde inbreuken op persoonsgegevens. |
| *Fase informatielevenscyclusmanagement:* **Gegevensbeveiliging** |
| *Gerelateerde kernelementen van de AVG:** Beveiliging van de verwerking
* Inbreuk in verband met persoonsgegevens
 |

Monitoren en handhaven

|  |
| --- |
| **Beoordeling van naleving privacywetgeving (REV)***Beheersingsdoelstelling:*De entiteit heeft een proces waarbij compliance met wet- en regelgeving met betrekking tot privacy bij voortduring wordt getoetst..  |
| *Fase informatielevenscyclusmanagement:* **Monitoren en handhaven** |
| *Beheersingsmaatregelen:* |  |
| REV01 | De entiteit heeft processen en procedures ingericht om:1. 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;
2. periodieke beoordelingen te documenteren, zoals interne auditplannen, auditrapporten, compliance checklists en aftekeningen (‘sign-offs’) van het management;
3. te rapporteren over de resultaten van deze conformiteitsbeoordelingen en daaruit voortvloeiende verbeteracties tijdig te implementeren;
4. op de hoogte te blijven van, en te anticiperen op (veranderingen in) toepasselijke wet- en regelgeving.
 | VV, V |
| *Gerelateerde kernelementen van de AVG:** Rechtmatigheid van de verwerking
 |

|  |
| --- |
| **Periodiek monitoren van privacybeheersingsmaatregelen (MON)***Beheersingsdoelstelling:* De entiteit toetst periodiek of getroffen beheersmaatregelen effectief zijn in relatie tot de privacyrisico’s van de entiteit. |
| *Fase informatielevenscyclusmanagement:* **Monitoren en handhaven** |
| *Beheersingsmaatregelen:* |  |
| MON01 | Het management van de entiteit evalueert de volgende zaken om de werking en toereikendheid van privacybeheersingsmaatregelen te waarborgen:1. control outputs, controlerapporten en deviaties;
2. opgetreden incidenten;
3. aanwezigheid bij (privacy-)trainingen en -evaluaties;
4. klachten en oplossing daarvan;
5. interne beoordelingen;
6. interne en externe auditrapporten;
7. audit/assurance-rapporten met betrekking tot privacybeheersingsmaatregelen bij derden/leveranciers;
8. 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 vaak dit gebeurt en met welke diepgang. | VV, V |
| MON03 | De entiteit heeft een proces ingericht om te waarborgen dat monitoring resulteert in herstel van tekortkomingen en continue verbetering. | VV, V |
| *Gerelateerde kernelementen van de AVG:** Rechtmatigheid van de verwerking
 |

# Deel 4. Capita Selecta

Toelichting

In de navolgende onderdelen wordt ingegaan op een aantal specifieke onderwerpen die in het kader van privacybeheersing bij sommige organisaties *bijzondere* aandacht verdienen. Achtereenvolgens komen aan de orde:

* Artificial Intelligence;
* Privacy by Design;
* Data localisation, internationale datatransfers, en DTIA’s;
* Anonimisering.

Deze thema’s zijn in meer of mindere mate gerelateerd aan bepaalde PCF-onderwerpen in deel 3, en kunnen in dat opzicht worden gezien als een verdieping op die onderwerpen. Bij elk thema is een korte toelichting opgenomen en een (niet-uitputtende) verwijzing naar relevante literatuur of achtergrondinformatie. Die is bedoeld om gebruikers van het PCF aanknopingspunten te geven om de te toetsen maatregelen voor deze thema’s waar nodig uit te breiden en/of beter toe te spitsen op de dienstverlening en de aard van de verwerkingen binnen een entiteit waar deze thema’s een specifiek van belang zijn.

Artificial Intelligence

In toenemende mate gebruiken organisaties kunstmatig intelligente algoritmische systemen (kortweg AI-systemen) in hun bedrijfsvoering. Deze systemen worden (ook) gebruikt ten behoeve van besluitvorming en kenmerken zich door hun autonome karakter en *learning ability.* Toepassing van AI-systemen brengt risico’s met zich mee voor het welzijn van personen wier gegevens door deze systemen worden verwerkt. Privacy moet worden gezien als één van de risico-categorieën die inherent is aan het gebruik van AI-systemen.

Alhoewel de AVG de term ‘Artificial Intelligence’ op geen enkele plaats expliciet noemt zijn er wel degelijk bepalingen binnen het wettelijk kader die door de toepassing van AI-systemen in het bijzonder aan betekenis winnen. Geautomatiseerde individuele besluitvorming (inclusief *profiling*) kan met AI-systemen worden bewerkstelligd, maar wordt in principe door de AVG niet toegestaan; de brede toepassingsmogelijkheden van AI-systemen en de grote hoeveelheden data die daarmee gemoeid zijn staan mogelijk op gespannen voet met wettelijke bepalingen rondom doelbinding en data-minimalisatie.

In dit verband is ook de AI Act van belang. Deze verordening is van toepassing op alle aanbieders en gebruikers van AI-systemen binnen de Europese Unie (EU), evenals op aanbieders buiten de EU waarvan de AI-systemen binnen de EU worden gebruikt. De AI Act is op 1 augustus 2024 in werking getreden en haar bepalingen worden gefaseerd van kracht. Voor organisaties betekent dit dat zij hun AI-systemen moeten evalueren en, indien nodig, aanpassen om te voldoen aan de nieuwe regelgeving door implementatie van maatregelen gericht op transparantie en risicobeheersing. Waar AI systemen persoonsgegevens verwerken, zullen organisaties vanzelfsprekend aan de bepalingen van zowel de AVG als de AI Act moeten voldoen. Alhoewel focus en reikwijdte van de twee verordeningen verschillen, zijn er duidelijke raakvlakken. In de navolgende tabel is daarvan een viertal belangrijke voorbeelden gegeven.

| **Artikel AVG** | **Onderwerp** | **Artikel AI Act**  | **Onderwerp** | **Relatie** |
| --- | --- | --- | --- | --- |
| Art. 5 | Beginselen gegevensverwerking | Art. 8, 10, 15  | Kwaliteit van data, transparantie en documentatie. | AI-systemen moeten voldoen aan de beginselen van doelbinding, dataminimalisatie en juistheid zoals vereist door de AVG. |
| Art. 9 | Verwerking van bijzondere gegevens | Art. 5, 10  | Verbod op gebruik van gevoelige data, tenzij onder voorwaarden. | Zowel AVG als AI Act reguleren strikt het gebruik van gevoelige data zoals ras, gezondheid of politieke opvattingen. |
| Art. 22 | Recht op menselijke tussenkomst bij geautomatiseerde besluitvorming | Art. 5, 13, 14  | Beperkingen op AI bij besluitvorming. | Zowel AVG als AI Act beschermen individuen tegen volledig geautomatiseerde beslissingen zonder menselijke tussenkomst. |
| Art. 35 | Data Protection Impact Assessment (DPIA) | Art. 9, 27  | Risicobeoordeling van AI-systemen. | Impact assessments zijn in veel gevallen ook vereist voor AI-systemen. |

Binnen NOREA doet de Kennisgroep Algorithm & Assurance onderzoek naar de mogelijke rol van de IT-auditor bij de toetsing van op Artificial Intelligence (AI) gebaseerde toepassingen. Deze Kennisgroep heeft *Guiding Principles* gepubliceerd, waarin (ook) aan privacyrisico’s gerelateerde *key questions* en voorbeelden van controlewerkzaamheden door de IT-auditor worden benoemd. Deze Guiding Principles vormen daarmee een solide uitgangspunt bij het beoordelen van privacybeheersing in de context van toepassing van AI-systemen binnen organisaties. Thema’s die in de privacygerelateerde key questions van de Guiding Principles aan de orde worden gesteld zijn onder andere:

* de uitvoering van een DPIA voor AI-systemen;
* ontwerp van AI-systemen waarbij de doelstelling van het AI-systeem duidelijk is omschreven en de verzameling van persoonsgegevens is in lijn met deze doelstelling;
* het, waar mogelijk, toepassen van anonimisering en pseudonimisering toe in het gebruik van het AI-systeem;
* de beperking van de verwerking van persoonsgegevens tot het noodzakelijk minimum voor de doelstelling van het AI-systeem;
* adequate governance en beveiliging van door het AI-systeem verwerkte gegevens.

De volledige Guiding Principles zijn beschikbaar op de NOREA-website.

|  |
| --- |
| ***Gerelateerde PCF-topics****:* DMI, ULI |
| ***Literatuursuggesties****:*NOREA Guiding Principles - *Trustworthy AI Investigations. Guiding principles for investigations of enterprise artificially intelligent algorithmic systems.**The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. EPRS | European Parliamentary Research Service, juni 2020. Verordening (EU) 2024/1689 van het Europees Parlement en de Raad (‘AI-Act’)Rijksoverheid, *Impact Assessment Mensenrechten en Algoritmes.*EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.* EPRS*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (study).* |

Privacy by Design

Er is brede consensus over het belang van vroegtijdige (en pro-actieve) aandacht voor privacy bij de ontwikkeling, ontwerp of aanschaf van diensten, producten, systemen en applicaties waarbij persoonsgegevens (zullen) worden verwerkt. De primaire afweging hierbij is dat mitigatie van privacyrisico’s een integraal aspect is van een ontwerpfase (in de brede zin van het woord), en daarmee in die ontwerpfase niet alleen efficiënter kan worden geïmplementeerd maar ook doeltreffender.

Minder duidelijk is hoe entiteiten dit principe van Privacy by Design (PbD) in de praktijk kunnen realiseren. De AVG vereist toepassing van PbD weliswaar expliciet (artikel 25), maar geeft behalve *pseudonimisatie* geen directe aanknopingspunten voor concrete te treffen maatregelen. De European Data Protection Board geeft op dat gebied meer duidelijkheid[[7]](#footnote-8). De Rijksoverheid (Ministerie van Justitie en Veiligheid) heeft een handleiding voor Privacy by Design (zie literatuurkader hieronder).

Wij noemen hierna een aantal best practices die gebaseerd zijn op de – binnen het privacy-vakgebied vaak gerefereerde- ‘zeven principes’ van PbD. Door deze best practices toe te passen kunnen organisaties PbD effectief implementeren, het vertrouwen van gebruikers vergroten, risico's minimaliseren en naleving van eisen uit wet- en regelgeving waarborgen.

Eerder in dit PCF is PbD aan de orde geweest in het onderdeel Gegevensbescherming door ontwerp en door standaardinstellingen (PBD).

*Kernprincipes als basis*

De zeven fundamentele principes van PbD, zoals proactief in plaats van reactief zijn en privacy als standaardinstelling verankeren, vormen het leidende kader. Proactief zijn betekent op privacyrisico’s anticiperen voordat ze zich voordoen, bijvoorbeeld door Privacy Impact Assessments (PIA’s) uit te voeren in de planningsfase van een project. Privacy by Default zorgt ervoor dat persoonlijke gegevens worden beschermd ‘als uitgangspunt’, dus zonder dat gebruikersacties nodig zijn om die bescherming te bewerkstelligen – denk aan een opt-out in plaats van een opt-in toestemmingsmodel. Organisaties moeten deze principes niet zien als louter nalevingsvereisten, maar als een best practice die in elke fase van productontwikkeling en operationele workflows wordt geïntegreerd.

*Dataminimalisatie*

Een van de meest effectieve PbD-technieken is dataminimalisatie – alleen die persoonsgegevens verzamelen die voor de doeleinden van de verwerking strikt noodzakelijk zijn. Technieken zoals anonimisering en pseudonimisering verminderen risico’s verder. Anonimisering verwijdert identificeerbare kenmerken uit gegevens, terwijl pseudonimisering identificatoren vervangt door omkeerbare codes, waardoor functionaliteit behouden blijft zonder ruwe persoonsgegevens bloot te geven. Deze methoden, ingebouwd in de systeemarchitectuur, beperken de impact van mogelijke datalekken en sluiten aan bij het PbD-principe van “end-to-end beveiliging”.

*Gebruikersgericht Ontwerp*

PbD geeft prioriteit aan keuzes voor gebruikers, wat transparantie en controle over persoonsgegevens met zich meebrengt. Best practices omvatten het ontwerpen van gebruikersvriendelijke intuïtieve middelen (zoals dashboards) waar gebruikers eenvoudig toestemmingen kunnen beheren en aanpassen, verzamelde gegevens kunnen bekijken en gegeven machtigingen kunnen intrekken. Als een betrokkenen dergelijke gedetailleerde opties krijgt versterkt dat diens vertrouwen en wordt beantwoord aan het PbD-principe van “zichtbaarheid en transparantie”.

*Technische Beveiliging*

Robuuste technische maatregelen zijn essentieel om PbD te operationaliseren. Toepassing van encryptie is een fundament, waarbij gegevens zowel in rust als tijdens verzending onleesbaar worden voor onbevoegden. Toegangscontroles, zoals op rollen gebaseerde rechten, zorgen ervoor dat alleen geautoriseerde medewerkers van persoonsgegevens kennis kunnen nemen. Daarnaast helpen regelmatige penetratietests en audits om kwetsbaarheden vroegtijdig te identificeren.

*Organisatorische Integratie*

PbD is niet alleen een technische activiteit, maar vooral een organisatorische verplichting. Het trainen van medewerkers in privacyprincipes en het bevorderen van samenwerking tussen afdelingen (bijv. juridisch, IT en ontwerp) zorgt voor consistente implementatie van privacybevorderende maatregelen. Het aanstellen van een coördinerende rol zoals een privacy officer kan verantwoordelijkheid centraliseren en coördinatie bevorderen, terwijl het integreren van PbD in agile ontwikkelingscycli – via privacy-sprints of checklists – een praktische invulling geeft in ontwikkeling en delivery.

Privacy by Design is een holistische benadering die het hanteren van een privacyprincipe combineert met uitvoerbare technieken. Door in een vroeg stadium data te minimaliseren, gebruikers centraal te stellen, systemen te beveiligen en een *privacy-first* cultuur te bevorderen kan een entitiet aantoonbaar maken privacybeheersing hoog in het vaandel te hebben, maar kan vertrouwen worden opgebouwd bij stakeholders.

|  |
| --- |
| ***Gerelateerde PCF-topics****:* PIA, SCO, SAT, PBD  |
|  |
| ***Literatuursuggesties****:*Privacy and Security by Design: An Enterprise Architecture Approach.EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.*Rijksoverheid/Ministerie van Justitie en Veiligheid, *Handleiding Privacy by Design*.Cavoukian, A. *Privacy by Design, The 7 Foundational Principles*. |

Data localisation, internationale datatransfers, en DTIA’s

Data localisation is het beleid of de praktijk waarbij gegevens fysiek worden opgeslagen en verwerkt binnen de grenzen van een specifiek land of een specifieke regio. Dit kan zijn opgelegd door wetgeving, organisatorisch beleid of technische vereisten. Het doel is vaak om controle te behouden over de data en te zorgen dat de omgang met deze data onderworpen blijft aan lokale wet- en regelgeving.

In relatie tot persoonsgegevens wordt data localisation vaak verondersteld een positieve factor te zijn. Door data binnen een bepaalde geografische regio te houden kunnen de betreffende overheden beter grip houden op hoe bedrijven omgaan met persoonlijke gegevens. Dit kan privacy versterken als die regio relatief strenge gegevensbeschermingswetten heeft. Het risico dat data wordt blootgesteld aan een (buitenlandse) verwerkingsomgeving met zwakkere privacywetten, surveillance door buitenlandse overheden, of dat datalekken zich uitstrekken buiten het eigen rechtsgebied wordt verkleind. Daarnaast voelen betrokkenen zich vaak comfortabeler als hun gegevens niet over grenzen heen gaan, zeker als het gaat om gevoelige informatie. Dit neemt niet weg dat ook gewezen wordt op het feit data data localisation in sommige gevallen juist een negatieve invloed op de bescherming van (persoons)gegevens kan hebben (bijvoorbeeld door een beperking om gebruik te maken van buitenlandse verwerkers als die strikter en zorgvuldiger omgaan met de verwerking van persoonsgegevens).

De AVG heeft geen expliciete eis voor data localisation, maar legt wel strikte regels op voor de overdracht van persoonsgegevens buiten de Europese Economische Ruimte (EER) of naar een internationale organisatie (AVG Hoofdstuk V). Persoonsgegevens mogen alleen worden overgedragen als het ontvangende land of de betreffende internationale organisatie een "passend beschermingsniveau" biedt. Of dit zo is kan worden vastgesteld op basis van adequaatheidsbesluiten van de Europese Commissie. Waar er voor een ‘derde land’ geen adequaatheidsbesluit is, kan een entiteit die desondanks persoonsgegevens naar een derde land of internationale organisatie wil overdragen, terugvallen op een aantal in de AVG genoemde alternatieven, zoals standaardcontractbepalingen (*Standard Contractual Clauses,* SCC’s) of bindende bedrijfsvoorschriften (*Binding Corporate Rules*): interne regels voor multinationals.

Door de strenge eisen aan internationale overdracht kiezen veel organisaties ervoor om persoonsgegevens binnen de EER te houden. Dit voorkomt juridische risico’s en vereenvoudigt naleving. Cloudproviders zoals AWS, Google Cloud en Microsoft Azure hebben datacenters in de EU opgezet om hieraan tegemoet te kunnen komen en "GDPR-compliant" diensten aan te bieden.

Met het Schrems II arrest maakte het Hof van Justitie van de Europese Unie (HvJEU) in 2020 niet alleen een einde aan het Privacy Shield voor overdracht van gegevens vanuit de EER naar de Verenigde Staten, maar bevestigde het tevens de geldigheid van SCCs als overdrachtsmechanisme. Daaraan werd echter wel een belangrijke voorwaarde gesteld: verwerkingsverantwoordelijken of verwerkers moeten per geval van overdracht vaststellen of de wetten en praktijken van het bestemmingsland een adequaat beschermingsniveau voor persoonsgegevens waarborgen, gelijkwaardig aan dat onder EU-recht (specifiek de AVG). Als het rechtskader van het bestemmingsland onvoldoende waarborgen biedt (bijvoorbeeld tegen gegevenstoegang door de overheid) moeten aanvullende maatregelen worden genomen om dit verschil in bescherming te overbruggen. Als dergelijke maatregelen niet mogelijk zijn of onvoldoende aanvullende bescherming kunnen garanderen mag de overdracht niet plaatsvinden.

Hoewel de term "Data Transfer Impact Assessment" niet in het Schrems II vonnis wordt gebruikt, komt de eis van een gedetailleerde, contextspecifieke analyse van de risico’s van de overdracht overeen met wat inmiddels in zekere zin is geformaliseerd als een ‘DTIA’. Latere richtlijnen van de EDPB (zie literatuurkader hieronder) bevelen expliciet het uitvoeren van dergelijke beoordelingen aan. De EDPB geeft een zesstappenproces voor het beoordelen van overdrachten, waaronder het in kaart brengen van gegevensstromen, het evalueren van de juridische omgeving van het derde land en het identificeren van aanvullende maatregelen. Deze richtlijnen operationaliseren de eisen van het HvJEU waardoor DTIA’s in feite voorgeschreven worden bij het gebruik van SCCs of vergelijkbare mechanismen onder artikel 46 van de AVG.

Bovendien eisen de bijgewerkte SCCs deze verplichting contractueel. Clausule 14 van de nieuwe SCCs vereist dat partijen een beoordeling van de wetten en praktijken van het derde land en eventuele aanvullende maatregelen documenteren. Hiermee wordt de uitvoering van een DTIA defacto vereist bij overdracht van persoonsgegevens naar derde landen of internationale organisaties zonder adequaatheidsbesluit.

|  |
| --- |
| ***Gerelateerde PCF-topics****:* DTR, TPD, TPA, STR |
| ***Literatuursuggesties:***EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.  |

Anonimisering

In de context van persoonsgegevens verwijst anonimisering naar het proces waarbij gegevens zodanig worden bewerkt dat ze niet langer herleidbaar zijn tot een specifiek individu, direct noch indirect. Het doel is om de identiteit van een persoon te beschermen door alle informatie die direct of indirect naar die persoon kan verwijzen (zoals naam, adres, geboortedatum of andere unieke kenmerken) te elimineren of onherkenbaar te maken.

Bij echte anonimisering is het belangrijk dat de gegevens permanent en onomkeerbaar worden losgekoppeld van het individu waarop ze betrekking hebben, zodat zelfs met aanvullende informatie de identiteit van die persoon niet meer kan worden achterhaald. Dit onderscheidt anonimisering van pseudonimisering, waarbij gegevens nog steeds gekoppeld kunnen worden aan een individu met behulp van een sleutel of extra informatie.

In de praktijk wordt anonimisering vaak toegepast om privacy te waarborgen, bijvoorbeeld bij het delen van dataverzamelingen voor onderzoek of statistische analyse. Anonimisering, alhoewel misschien lastig te bewerkstelligen, maakt compliancevraagstukken echter wel eenvoudiger. Anonieme gegevens vallen namelijk niet onder de regels van AVG, omdat ze niet langer binnen de definitie van persoonsgegevens in de context van de wet vallen.

**Technieken voor anonimisering**

*Maskering*

Bij maskeren worden specifieke delen van de gegevens verborgen of vervangen door neutrale tekens (zoals sterretjes of X'en). Bijvoorbeeld: een telefoonnummer `06-12345678` wordt `06-XXXX5678`.

Maskering kan bijvoorbeeld worden toegepast voor gegevens die slechts gedeeltelijk herkenbaar hoeven te blijven, zoals bij klantenservice (waar een medewerker een deel van het nummer ziet om een klant te verifiëren).

*Generalisatie*

Bij generalisatie worden gegevens minder specifiek gemaakt door details te verwijderen of een categorisering te hanteren. Bijvoorbeeld: een exacte geboortedatum "15-03-1985" wordt "1985" of "1980-1990".

Generalisatie kan bijvoorbeeld worden toegepast voor statistische analyses waarbij precieze individuele gegevens niet nodig zijn, zoals demografische rapportages.

*Differentiële privacy*

Bij differentiële privacy wordt willekeurige "ruis" toegevoegd aan de gegevens of de resultaten van een analyse, zodat het onmogelijk wordt om te bepalen of een specifiek individu in de dataset zit. Dit gebeurt vaak met wiskundige algoritmes (zoals Laplace- of Gauss-mechanismen).

Differentiële privacy kan worden toegepast voor grootschalige datasets waarbij privacy gegarandeerd moet worden, maar statistische inzichten behouden blijven (bijv. bij volkstellingen of machine learning). Het biedt een wiskundige garantie voor privacy en is bestand tegen aanvallen met (aanvullende) gegevens uit externe datasets. Daat staat tegenover dat de implementatie van differentiële privacy complex is om te implementeren en de balans tussen ruis en nauwkeurigheid lastig te vinden is. Te veel ruis maakt resultaten onbruikbaar.

*K-anonimiteit*

K-anonimiteit zorgt ervoor dat elk individu in een dataset niet te onderscheiden is van minstens \*k-1\* andere personen op basis van bepaalde kenmerken (quasi-identificatoren zoals leeftijd, geslacht, postcode). Bijvoorbeeld: als k=3, moeten er minstens 3 mensen in de dataset zijn met dezelfde combinatie van kenmerken.

K-anonimiteit is geschikt voor verzamelingen (persoons)gegevens die gedeeld worden met derden, zoals onderzoeksinstanties, waarbij heridentificatie voorkomen moet worden. K-anonimiteit wordt over het algemeen beschouwd als een eenvoudiger techniek dan differentiële privacy en als effectief tegen simpele heridentificatiepogingen.

In de praktijk bovengenoemde technieken vaak gecombineerd, al naar gelang de doelstelling en de aard van de verwerking.

|  |
| --- |
| ***Gerelateerde PCF-topics****:* DDA, PBD, TPD |
| ***Literatuursuggesties:***EDPB, *Guidelines 01/2025 on Pseudonymisation.*ENISA, *Pseudonimisation techniques and best practices*.ISO 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques.* |

# Bijlage 1. Relatie PCF - AVG

**Relatie tussen kernelementen AVG, artikelen AVG, en PCF-topics**

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)
* Minimalegegevensverwerking (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)
* Periodiek monitoren van privacybeheersings-maatregelen (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 privacybeheersings-maatregelen (MON)
 |
| Rechten van de betrokkene | Artikel 12 - Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkeneArtikel 13 - Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameldArtikel 14 - Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregenArtikel 15 - Recht van inzage van de betrokkene Artikel 16 - Recht op rectificatieArtikel 17 - Recht op gegevenswissing (‘recht op vergetelheid’) Artikel 18 - Recht op beperking van de verwerkingArtikel 19 - Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperkingArtikel 20 - Recht op overdraagbaarheid van gegevens  | * Gebruik en beperking (URE)
* Verzoeken van betrokkenen (DSR)
* Toestemmingsraamwerk (CFR)
* Privacyverklaring (PST)
 |
| Recht op overdraagbaarheid van gegevens | Artikel 20 - Recht op overdraagbaarheid van gegevens | * Verzoeken van betrokkenen (DSR)
 |
| Gegevensbescherming door ontwerp / door standaardinstellingen | Artikel 25 - Gegevensbescherming door ontwerp en door standaardinstellingen | * Risicomanagement (RMA)
* Afbakening van rollen en verantwoordelijk-heden (RRE)
* Competenties medewerkers (SCO)
* Minimale gegevensverwerking (DMI)
* Doelbinding (ULI)
* Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) (PBD)
* Verzoeken van betrokkenen (DSR)
* Verwijdering, vernietiging en anonimisatie (DDA)
 |
| Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker | Artikel 24 - Verantwoordelijkheid van de verwerkingsverantwoordelijke Artikel 28 - Verwerker  | * Afbakening van rollen en verantwoordelijk-heden (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)
* Afbakening van rollen en verantwoordelijk-heden (RRE)
* Verwijdering, vernietiging en anonimisatie (DDA)
* Verzoeken van betrokkenen (DSR)
* 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 autoriteitArtikel 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 gegevensbeschermingArtikel 38 - Positie van de functionaris voor gegevensbeschermingArtikel 39 - Taken van de functionaris voor gegevensbescherming | * Afbakening van rollen en verantwoordelijk-heden (RRE)
* Competenties medewerkers (SCO)
 |
| Doorgiften van persoonsgegevens aan derde landen of internationale organisaties | Artikel 44 - Algemeen beginsel inzake doorgiftenArtikel 45 - Doorgiften op basis van passende waarborgenArtikel 46 - Transfers subject to appropriate safeguardsArtikel 47 - Bindende bedrijfsvoorschriftenArtikel 48 - Niet bij Unierecht toegestane doorgiften of verstrekkingenArtikel 49 - Afwijkingen voor specifieke situatiesArtikel 50 - Internationale samenwerking voor de bescherming van persoonsgegevens | * Afbakening van rollen en verantwoordelijk-heden (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 in 2017 beschreven werd in de scriptie van Koetsier en Ougajou en de daaropvolgende
 [publicatie in *de IT-Auditor*](https://www.norea.nl/uploads/bfile/36520a94-6121-4884-a3fa-fc6d4a372e98).

De 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 GAPP5-principes en de OECD6-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.

5 GAPP, An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009.
6 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/data-eigenaren;
* 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 verbeteren.

# Bijlage 3. PCF en ISO-standaarden

Deze bijlage geeft enige verduidelijking aan de relatie tussen het PCF en een aantal ISO-standaarden op het gebied van informatiebeveiliging en privacy. Achtereenvolgens zijn dat ISO 27001/27002, ISO 27701, ISO 27018, en ISO 29100.

ISO 27001/27002

ISO 27001[[8]](#footnote-9) specificeert een standaard voor een informatiebeveiligingsmanagementsysteem (ISMS). In aansluiting daarop geeft ISO 27002 een verzameling richtlijnen en best practices op het gebied van informatiebeveiligingsmanagement. Gemakshalve refereren we in deze bijlage aan de combinatie van beide als als ‘ISO 27001’).

Alhoewel de meest recente versie van ISO 27001 de term ‘privacy’ in de titel draagt, komen de woorden ‘privacy’ en ‘persoonsgegevens’ in de tekst van de standaard 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 in ISO 27001 ingesloten. Ook de beheersmaatregelen in de bijlage van ISO 27001 noemen persoonsgegevens slechts op een enkele plek expliciet. Maatregel A.5.34 uit Bijlage A luidt als volgt:

*“De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.”*

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 dan worden gebruikt om een adequate opzet en implementatie van het gestelde in A.5.34 vast te stellen. De praktische uitvoerbaarheid daarvan is echter twijfelachtig. Aan ISO 27001 worden dan 32 beheersdoelstellingen uit het PCF ‘toegevoegd’ om vast te stellen of aan één eis van ISO 27001 wordt voldaan.

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 maatregel zoals verwoord in A.5.34. 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 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 |
| **Control objective****/doelstelling** | *(In tegenstelling tot de vorige versie van ISO 27001 noemt de 2022-versie geen beheersingsdoelstellingen meer)* | 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. |
| **Control/****beheersmaatregel** | A.6.8 De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings-gebeurtenissen tijdig via passende kanalen kan melden.  | **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. |

Bij een dergelijke aanpak is het uiteraard 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.6.8 (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

In aanvulling op ISO 27001 en 27002 is ISO 27701[[9]](#footnote-10) als een specifieke standaard gepubliceerd voor het inrichten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor privacy-informatie (Privacy Information Management System, PIMS).

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 27018

ISO 27018[[10]](#footnote-11) specificeert beheersingsdoelstellingen en -maatregelen voor de bescherming van persoonsgegevens in een *public cloud* omgeving. De standaard is bedoeld voor organisaties die (contractueel) cloud-diensten aanbieden aan andere organisaties en daarbij als verwerkers van persoonsgegevens optreden.

ISO 29100

ISO/IEC 29100[[11]](#footnote-12) geeft een standaard voor een privacyraamwerk op hoog niveau, dat organisaties in staat stelt 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 algemeen geformuleerd, en als een basis te beschouwen voor de nadere uitwerking in ISO 27701 en ISO 27018. In relatie tot het PCF kan worden gesteld dat de principes in ISO 29100 sterk gerelateerd zijn aan de topics en beheersingsdoelstellingen van het PCF. In de tabel in de volgende paragraaf is deze relatie verduidelijkt.

Cross-reference tussen PCF en ISO

In onderstaande tabel is een indicatieve cross-reference gemaakt van de onderwerpen uit het PCF met bovengenoemde ISO standaarden (met uitzondering van ISO 27018 aangezien die is gericht op een zeer specifieke groep entiteiten).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tag (PCF) | Topic (PCF) | Gerelateerde eisen en beheersingsmaatregeken ISO 27001:2022 | Gerelateerde beheersmaatregelen ISO 27701:2019 | Gerelateerde principes ISO 29100:2011 |
| PPO | Privacybeleid | A.5.1Clause: 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 specificationOpenness, transparency and noticeAccountability |
| RRE | Afbakening van rollen en verantwoordelijkheden | A.5.2, A.5.3, A.5.4, A.6.5Clause: 5.1, 5.3 | 5.2.1A.7.2.7, B.8.2.1, B.8.2.6 | Accountability |
| PDI | Identificatie en classificatie van persoonsgegevens | A.5.12, A.5.13 | 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.5.7, A.8.8Clause: 6.1.1, 6.1.2, 6.1.3, 8.2 | 5.4.1.2 | Accountability |
| PIA | Data protection impact assessments | A.5.7, A.5.8, A.5.35, A.8.8, A.8.27, A.8.32Clause: 6.1.2, 6.1.3, 8.2 | 5.4.1.2A.7.2.5 | Accountability |
| PIB | Beheer van privacyincidentenen inbreuken | A.5.25 t/m A.5.28, A.6.8, A.8.12 |  | Accountability |
| SCO | Competenties mede-werkers | A.6.3Clause: 7.2 |  | Accountability |
| SAT | Bewustwording en training medewerkers | A.6.3Clause: 7.3 |  | Accountability |
| LRC | Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten | A.5.31Clause: 4.2 |  | Privacy compliance |
| PST | Privacyverklaring | - | A.7.3.1, A.7.3.2, A.7.3.3 | Openness, transparency and notice |
| CFR | Toestemmingsraamwerk | - | A.7.2.3, A.7.2.4, A.7.3.4 | Consent and choice |
| DMI | Minimale gegevensverwerking | - | 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 | Privacyarchitectuur (Gegevens-bescherming door ontwerpen door standaard-instellingen) | A.5.8, A.8.25, A.8.27, A.8.28, A.8.32 | A.7.4 | Use, retention and disclosure limitation |
| DRE | Bewaren van gegevens | A.8.10 | A..7.4.7 | Use, retention and disclosure limitation  |
| DDA | Verwijdering, vernietiging en anonimiseren | A.8.10, A.8.11 | 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  |
| DSR | Verzoeken van betrokkenen | - | A.7.3.3, A.7.3.6, A.7.3.7, A.7.3.8, A.7.3.9 | Individual participation and access / Accuracy and quality |
| ACD | Juistheid en volledigheid van gegevens | - | A.7.4.3 | Accuracy and quality |
| TPD | Verstrekking aan derden en registratie | A.8.3, A.5.14 | A.7.5.1, A.7.5.3, A.7.5.4 | Use limitation |
| TPA | Overeenkomstenmet derden | A.5.19 t/m A.5.22 | 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.5.14 | 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, A.5.15, A.5.18, A.8.3 t/m A.8.5 |  | Information security |
| IAM | Identiteit en toegangsbeheer | A.5.15 t/m A.5.18, A.6.6, A.8.3 t/m A.8.5 |  | Information security |
| STR | Veilige gegevensoverdracht | A.5.14, A.8.20 t/m A.8.23 | A.7.4.9, B.8.4.3 | Information security |
| ENC | Versleuteling en eindpuntbeveiliging | A.8.1, A.8.11, A.8.24 |  | Information security |
| LOG | Registreren van toegang | A.8.15 |  | Information security |
| REV | Beoordeling van compliance met privacywetgeving | Clause: 9, 10A.5.31, A.5.36 |  | Privacy compliance |
| MON | Periodiek monitoren van privacybeheersingsmaatregelen | Clause 9, 10A.8.16, A.5.35 |  | Privacy compliance |

In onderstaande tabel is volledigheidshalve weergegeven aan welke onderdelen van ISO 27001 en ISO 27701 de privacyonderwerpen uit het PCF gerelateerd zijn.

|  |
| --- |
| Relatie tussen ISO 27001, ISO 27701 en PCF onderwerpen |
| ISO 27001:2013 | **Onderwerp** | **PCF** |
| Clause 4 | Context van de organisatie | PPO, LRC |
| Clause 5 | Leiderschap | PPO |
| Clause 6 | Planning | RMA |
| Clause 7 | Ondersteuning | SCO |
| Clause 8 | Uitvoering | RMA, PIA |
| Clause 9 | Evaluatie van de prestaties | REV, MON, RMA |
| Clause 10 | Verbetering | REV, MON |
| (*door de veranderde structuur in ISO 27001 versie 2022 is een relatie tussen de onderwerpen van het PCF en de hoofdonderwerpen van Bijlage A van ISO 27001 niet meer zinvol)* |
| ISO 27701:2021 | **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, DSR  |
| 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 | DSR, STR |
| B.8.5 | PII Sharing, transfer and disclosure | DTR, TPA |
|  |  |  |

1. An Executive Overview of GAPP: Generally Accepted Privacy Principles, 2009. [↑](#footnote-ref-2)
2. Security and Privacy Controls for Federal Information, Systems and Organizations, NIST SP800-R53 Privacy Control Catalog, 2013 [↑](#footnote-ref-3)
3. Het NOREA Raamwerk Privacy Audit, 2005, Addendum Norea Privacy Audit bij Richtlijn 3600n, 2017 [↑](#footnote-ref-4)
4. European Privacy Seal EuroPriSe, 2008 [↑](#footnote-ref-5)
5. Voor het onderdeel ‘Gegevensbeveiliging’ geeft het PCF geen beheersingsmaatregelen. De reden daarvoor zijn in deel 3 (bij het onderdeel ‘Gegevensbeveiliging’ uiteengezet. [↑](#footnote-ref-6)
6. Hierna aangeduid als ‘privacy officer’. [↑](#footnote-ref-7)
7. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 [↑](#footnote-ref-8)
8. ISO/IEC 27001:2022 Informatiebeveiliging, cybersecurity en bescherming van de privacy – Managementsysteem voor informatiebeveiliging – Eisen [↑](#footnote-ref-9)
9. ISO/IEC 27701:2021 Veiligheidstechnieken - Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement - Eisen en richtlijnen. [↑](#footnote-ref-10)
10. ISO/IEC 27018:2020 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [↑](#footnote-ref-11)
11. ISO/IEC 29100:2024 Information technology -- Security techniques -- Privacy framework [↑](#footnote-ref-12)