# Handleiding Privacy by Design

**Auteurs**: Nine Bennink LL.M., Hadassah Drukarch
**Versie**: 1.0
**Datum**: 26-9-2023
**Opdrachtgever**: Ministerie van Justitie en Veiligheid
**Contactpersoon**: Pauline Verhaak, p.m.verhaak@minjenv.nl

# Inhoud

# Managementsamenvatting

Voor u ligt de Handleiding Privacy by Design (PbD). De Nederlandse benaming voor 'PbD' is 'privacy door ontwerp'. Dit houdt kort gezegd in dat u privacy en gegevensbescherming meeneemt als eisen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt. Het uitgangspunt van PbD is in de Algemene verordening gegevensbescherming (AVG) neergelegd als een plicht voor de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke moet kunnen aantonen dat met PbD rekening is gehouden.

Wat u moet doen om invulling te geven aan het uitgangspunt van PbD is afhankelijk van het concrete geval. Deze Handleiding is ondersteunend bij de beslissingen die u dient te maken rondom het invulling geven aan PbD in een concreet geval.

De Handleiding is dan ook geen verplicht instrument en ook niet te beschouwen als een 'afvinklijstje'.

Het toepassingsgebied van de Handleiding is breed. Deze Handleiding kan worden gebruikt als u zelf producent bent van een product, dienst of toepassing die is gebaseerd op de verwerking van persoonsgegevens of als u zelf verantwoordelijk bent voor beleid. Ook kan deze Handleiding worden gebruikt wanneer een derde producent is of verantwoordelijk voor het beleid, of wanneer er sprake is van een openbare aanbesteding. Deze Handleiding is ondersteunend aan al deze processen om de afweging te maken wat er in een concreet geval verwacht wordt van bijvoorbeeld een proceseigenaar, een systeemarchitect of van een derde partij.

Deze Handleiding is voorts niet beperkt tot een bepaalde doelgroep of een bepaalde manier van werken (bijvoorbeeld alleen agile of alleen waterfall software ontwikkeling), maar geschikt voor iedereen die te maken heeft met de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt. De manier waarop u te werk gaat is voor het gebruik van deze Handleiding irrelevant.

U hoeft niet de hele Handleiding te lezen om het document te begrijpen en toe te passen. De Handleiding is namelijk opgedeeld in drie delen die afzonderlijk van elkaar kunnen worden bekeken.

Onderdeel I 'praktische handvatten inbedding PbD' is het praktische deel van de Handleiding. Hierin staan *best practices* en ontwerpstrategiëen. Dit onderdeel kan worden gebruikt zonder het bestuderen van onderdelen II en III van de Handleiding PbD. U kunt hier concrete handvatten vinden om PbD toe te passen. Onderdeel II 'theoretische verdieping rondom PbD' is de theoretische verdieping van Onderdeel I. Door dit (gedeeltelijk) door te nemen, ontstaat er meer begrip over de wijze waarop u over PbD zou kunnen nadenken en wie vanuit welke rol (deels) verantwoordelijk is voor de invulling van PbD in een concreet geval. Hier wordt ook de link gelegd met de AVG en de daarin opgenomen plicht van de verwerkingsverantwoordelijke. Onderdeel III 'aanvullende bronnen en overzichten' bevat achtergrondinformatie. In paragraaf 1.2. van hoofdstuk 1 van de Handleiding is een leeswijzer opgenomen.

Tot slot is van belang dat dit document een levend document is en niet te beschouwen als een 'afvinklijstje' dat nu klaar is. De opstellers van de Handleiding nodigen u uit de Handleiding aan te vullen met uw eigen *best practices* en het gesprek over PbD met elkaar te gaan voeren.

# 1. Inleiding

## 1.1. Scope en doel handleiding

Deze handleiding gaat over Privacy by Design (hierna: "PbD") en legt de focus op PbD zoals dat in de Algemene verordening gegevensbescherming (hierna: "AVG") is opgenomen. Deze handleiding is ook toepasbaar voor PbD buiten het toepassingsbereik van de AVG, onder meer voor verwerkingen onder de Wet politiegegevens (hierna: "Wpg") en Wet justitiële en strafvorderlijke gegevens (hierna: "Wjsg"). PbD is niet alleen opgenomen in de AVG, maar ook in andere wettelijke regelingen. De kern van PbD is overal min of meer gelijk, maar tegelijkertijd kennen de wettelijke regelingen ook verschillen. Dit betekent enerzijds dat de handleiding toepasbaar is voor verwerkingen buiten het AVG-regime, en anderzijds dat de handleiding focus legt op PbD zoals opgenomen in de AVG. Verder komen de PbD-ontwerpstrategieën aan de orde.[1] De handleiding geeft handvatten om PbD concreter te kunnen toepassen.

Met het oog op de dynamische aard van PbD, worden alle gebruikers van deze handleiding actief aangemoedigd om dit document als een living document te beschouwen en up-to-date te houden, bijvoorbeeld door bij de hiervoor genoemde contactpersoon *best practices* voor de databank van goede voorbeelden aan te leveren en nieuwe ontwikkelingen te signaleren.

### De scope

| Onderdeel | In scope | Buiten scope |
|---|---|---|
| Theorie | Theorie PbD<br>Ontwerpstrategieën PbD | Uitleg AVG[2]<br>Privacy by default<br>DPIA |
| Praktijk | PbD *best practices* | |
| Techniek | | Beschrijving technische keuzes |
| Overig | | Archiving by design<br>Security by design |

### De doelgroep

PbD is een verantwoording van elke medewerker die zich bezighoudt met de ontwikkeling van nieuwe of vernieuwde processen, applicaties, etc. waarbij persoonsgegevens (in de toekomst zullen) worden verwerkt of waarbij de verwachting bestaat dat persoonsgegevens zullen worden verwerkt, zoals privacy officers, proceseigenaren, verschillende groepen van architecten, developers en het bestuur/de directie. Deze handleiding richt zich op deze doelgroep. Zie hierover verder hoofdstuk 7 van de handleiding.

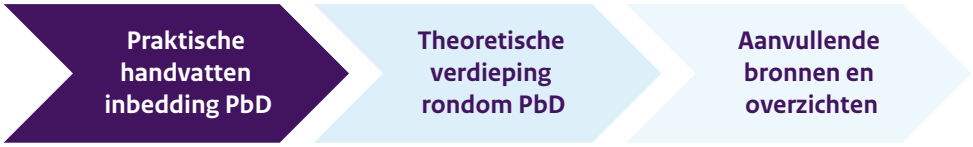
## 1.2. Leeswijzer

De handleiding is opgebouwd uit de volgende drie onderdelen die los van elkaar kunnen worden bestudeerd. Het is dus niet nodig om in alle gevallen alles te bestuderen.

1 Deze ontwerpstrategieën worden beschreven in Het Blauwe Boekje geschreven door dhr. dr. J.H. Hoepman, 27 januari 2020.

2 Waar de basisprincipes en grondslagen uit de AVG van belang zijn, word verwezen naar de handleiding AVG en UAVG: https://open.overheid.nl/repository/ronl-dd12795b-eaa8-4e23-b552-96ef285cb9ad/1/pdf/Handleiding%20Algemene%20verordening%20gegevensbescherming.pdf.

De kern van de handleiding wordt gevormd door onderdeel I. Onderdeel I is het praktische deel van de handleiding.
In onderdeel II wordt  voor achtergrondinformatie verwezen naar onderdeel II.
Onderdeel III als bronnenoverzicht, definitielijst, en omvat aanvullende (schematische) overzichten.




Hierna volgt een verduidelijking van elk onderdeel:

### Onderdeel I: praktische handvatten inbedding PbD

| Het doel van onderdeel I is om de lezer: | O.b.v. onderdeel I, is de lezer in staat om: |
|---|---|
| **HOOFDSTUK 2** | |
| inzicht te geven in de PbD ontwerpstrategieën. | • te begrijpen welke ontwerpstrategieën voor de praktische inbedding van PbD bestaan;<br>• te begrijpen wanneer de toepassing hiervan wenselijk is;<br>• de ontwerpstrategieën te onderscheiden. |
| middels de PbD beslisboom praktische handvatten te geven om de PbD ontwerpstrategieën te doorlopen. | middels de PbD beslisboom de PbD ontwerpstrategieën te doorlopen en op basis daarvan per geval een selectie te maken van de meest relevante PbD ontwerpstrategieën. |
| inzicht te geven in de verhouding tussen de PbD ontwerpstrategieën en de privacybeginselen uit de AVG. | te begrijpen hoe de PbD ontwerpstrategieën zich verhouden tot de privacybeginselen uit de AVG en daarmee begrip te kweken voor het belang en de praktische noodzaak voor de inbedding van PbD. |
| **HOOFDSTUK 3** | |
| een stappenplan te bieden voor de praktische inbedding van PbD. | met het stappenplan PbD in de praktijk in te bedden binnen de eigen organisatie en processen. |
| een toolkit te bieden waarmee praktische beslissingen kunnen worden genomen omtrent de inbedding van PbD. | met de toolkit beslissingen te nemen om PbD in de praktijk in te bedden binnen de eigen organisatie en processen. |
| inzicht te bieden in een niet-limitatieve opsomming van *best practices* voor de praktische inbedding van PbD. | • de praktische inbedding van PbD binnen de eigen organisatie en processen verder vorm te geven op basis van bestaande *best practices*<br>• inspiratie op te doen om zelf nieuwe *best practices* te ontwikkelen. |

### Onderdeel II: theoretische verdieping rondom PbD.

| Het doel van onderdeel II is om de lezer: | O.b.v. onderdeel II, is de lezer in staat om: |
|---|---|
| **HOOFDSTUK 4** | |
| een introductie tot PbD en de bescherming van persoonsgegevens te geven. | te begrijpen wat de wettelijke verplichting tot PbD inhoudt en waarom deze belangrijk is voor de bescherming van persoonsgegevens. |
| inzicht te bieden in de theoretische verhouding tussen PbD en de privacybeginselen uit de AVG, met name de principes van rechtmatigheid en behoorlijkheid. | te begrijpen hoe PbD en de privacybeginselen uit de AVG in theorie met elkaar samenhangen en welke rol behoorlijkheid en rechtmatigheid hierin spelen. |
| **HOOFDSTUK 5** | |
| uitleg te bieden over de verschillende theoretische aspecten die relevant zijn voor de praktische implementatie van PbD, waaronder de PbD vuistregels en de systeemlevenscyclus. | • te begrijpen welke aspecten onderdeel vormen van de praktische implementatie van PbD;<br>• te begrijpen welke vuistregels gevolgd moeten worden om PbD in de praktijk te implementeren;<br>• te begrijpen wat de systeemlevenscyclus van PbD is. |
| **HOOFDSTUK 6** | |
| te voorzien in een diepere theoretische onderbouwing rondom de privacybeginselen uit de AVG. | te begrijpen welke privacybeginselen de AVG voorschrijft en wat deze betekenen voor de verwerking van persoonsgegevens. |
| een overzicht te bieden van de relevante vragen die gesteld kunnen worden om de privacybeginselen uit de AVG in de praktijk te toetsen. | in de praktijk te toetsen of in een bepaald geval aan de privacybeginselen van de AVG wordt voldaan. |
| uitleg te bieden rondom de noodzakelijkheidstoets bij de verwerking van persoonsgegevens en de relevante aspecten die hierbij in overweging genomen moeten worden. | te begrijpen wat 'noodzakelijkheid' betekent in het kader van gegevensverwerkingen en die noodzakelijkheidstoets te kunnen uitvoeren. |
| **HOOFDSTUK 7** | |
| een overzicht te bieden van de rollen die relevant zijn in het kader van praktische inbedding van PbD binnen de eigen organisatie en processen. | In staat om relevante personen binnen de organisatie aan te wijzen om de implementatie c.q. (betere) inbedding van PbD in de praktijk te realiseren. |

### Onderdeel III: aanvullende bronnen en overzichten

## 1.3. Proclaimer

Hieronder volgen enkele punten van aandacht:

- deze handleiding is geen 'afvinklijstje' omdat PbD vereist dat de bescherming van privacy gedurende de gehele cyclus van systemen, applicaties, processen, beleid en producten wordt meegenomen;
- alle voorbeelden die zijn opgenomen in de handleiding hebben een informatief doel en zijn niet afgestemd. Het zijn fictieve voorbeelden;
- de genoemde *best practices* zijn niet in alle gevallen passend;
- deze handleiding omvat geen concrete technische keuzes. Waar relevant, worden technische maatregelen als voorbeelden genoemd. Een verdere uitwerking van deze technische maatregelen valt buiten de scope van deze handleiding.

Bij twijfel dient u altijd contact op te nemen met de Privacy Officer (hierna: "PO").

# DEEL I | Praktische handvatten inbedding PbD

# 2. PbD ontwerpstrategieën: uitleg en concrete stappen

## 2.1. PbD ontwerpstrategieën: algemeen

Om handvatten te geven voor het doorvoeren van PbD tijdens het ontwerp en de verdere levensduur van systemen, applicaties, processen, beleid en producten, is een aantal ontwerpstrategieën ontwikkeld, neergelegd en uitgelegd in 'Het Blauwe Boekje', gratis te vinden en te downloaden via internetzoek-machines. [3] Het gaat om de volgende ontwerpstrategieën:

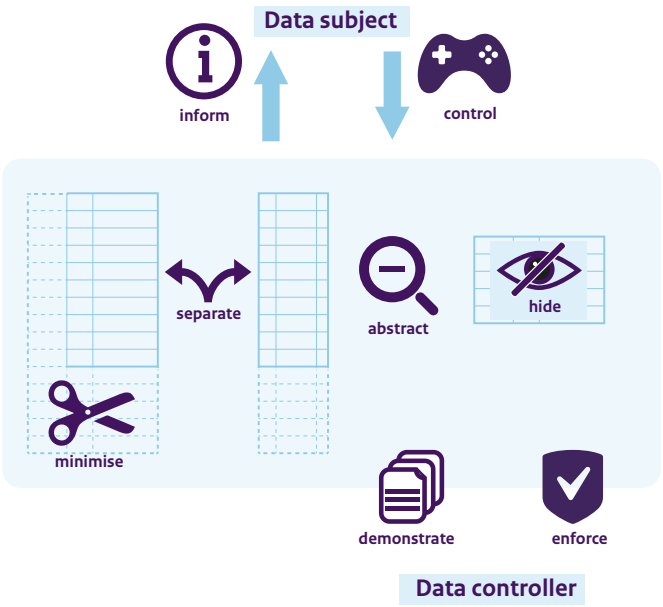
- Minimaliseer
- Scheid
- Verberg
- Onttrek
- Informeer
- Beheers
- Handhaaf
- Toon aan

Zie voor achtergrondinformatie over de **theoretische inkadering van PbD** paragrafen 4.1, 4.3, 5.1 en 5.2 van deze handleiding.

Deze ontwerpstrategieën dienen de implementatie van privacy in de praktijk in de verhouding tussen de verwerkingsverantwoordelijke en de betrokkene, zoals in figuur 2.1 is afgebeeld.

3 De privacy by Design ontwerpstrategieën zoals gebruikt in dit Framework zijn ontworpen door prof. Jaap Henk Hoepman van de Radboud Universiteit Nijmegen en zijn onder andere toegepast door de European Network Security Agency (ENISA) en de Zweedse gegevensbeschermingsautoriteit. Daarom worden ze gezien als maatgevend op dit gebied en het meest 'state of the art' in het overbruggen van de juridische wereld en de IT-wereld. Zie Hoepman (2013), *Privacy design strategies*; en Colesky, Hoepman and Hillen (2016), *A Critical Analysis of Privacy Design Strategies*.

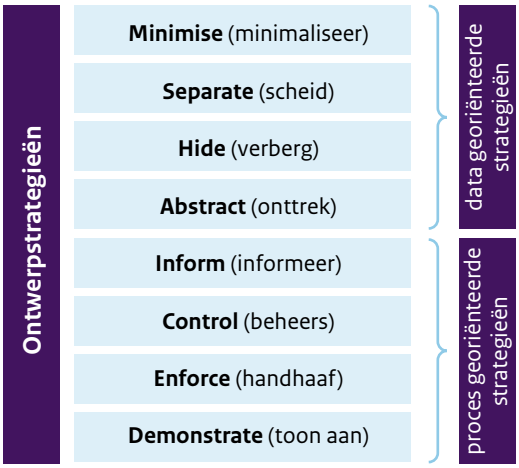
**Figuur 2.1.** Ontwerpstrategieën in de verhouding verwerkingsverantwoordelijke (data controller) - betrokkene (data subject).




## 2.2. Data en proces georiënteerde PbD ontwerpstrategieën

De PbD ontwerpstrategieën kunnen onderverdeeld worden in **data en proces georiënteerde ontwerpstrategieën** (zie figuur 2.2).

**Figuur 2.2.** PbD data en proces georiënteerde ontwerpstrategieën.




De **data georiënteerde strategieën** richten zich op de verwerking van persoonsgegevens zelf en zijn daardoor technisch van aard. De data georiënteerde strategieën betreffen met name technische aspecten van de verwerking van persoonsgegevens.

**VOORBEELD**
Voor de aanvraag van gesubsidieerde rechtshulp moet worden nagegaan of een persoon onder of boven het drempelbedrag zit. Hierbij wordt een inkomenstoets gedaan bij de belastingdienst. In plaats van het precieze inkomen te tonen, wordt alleen getoond of iemand onder of boven het dempelbedrag zit.

De **proces georiënteerde strategieën** zijn organisatorische maatregelen. Deze maatregelen zien op de organisatie en de mens daarin en niet op de technische maatregelen die kunnen worden getroffen, bijvoorbeeld het verstrekken van informatie aan betrokkenen.

**VOORBEELD**
Zo informeert een organisatie  via de privacyverklaringen de betrokkenen over hun rechten met betrekking tot hun gegevens, zoals het recht op inzage, correctie of verwijdering, etc. en biedt het een mechanisme, bijvoorbeeld via een contactformulier, waarmee de betrokkenen deze rechten kunnen uitoefenen. Het betreft hier de proces georiënteerde strategie 'beheers'.

Aan deze ontwerpstrategieën kan invulling gegeven worden door middel van een aantal tactieken (zie tabel 2.1). Deze tactieken zijn echter niet zwart wit: er moet ook worden gekeken naar de ontvanger/gebruiker van de persoonsgegevens en de praktijk van de organisatie. Ter illustratie: een medewerker die over een specifieke casus informatie opvraagt dient soms juist concrete data te ontvangen en geen data met ruis, conform de aanvraag. Een onderzoeker die een analyse wil maken van een proces in zijn algemeenheid, kan wellicht wel met gegroepeerde, geminimaliseerde en data met ruis uit de voeten.

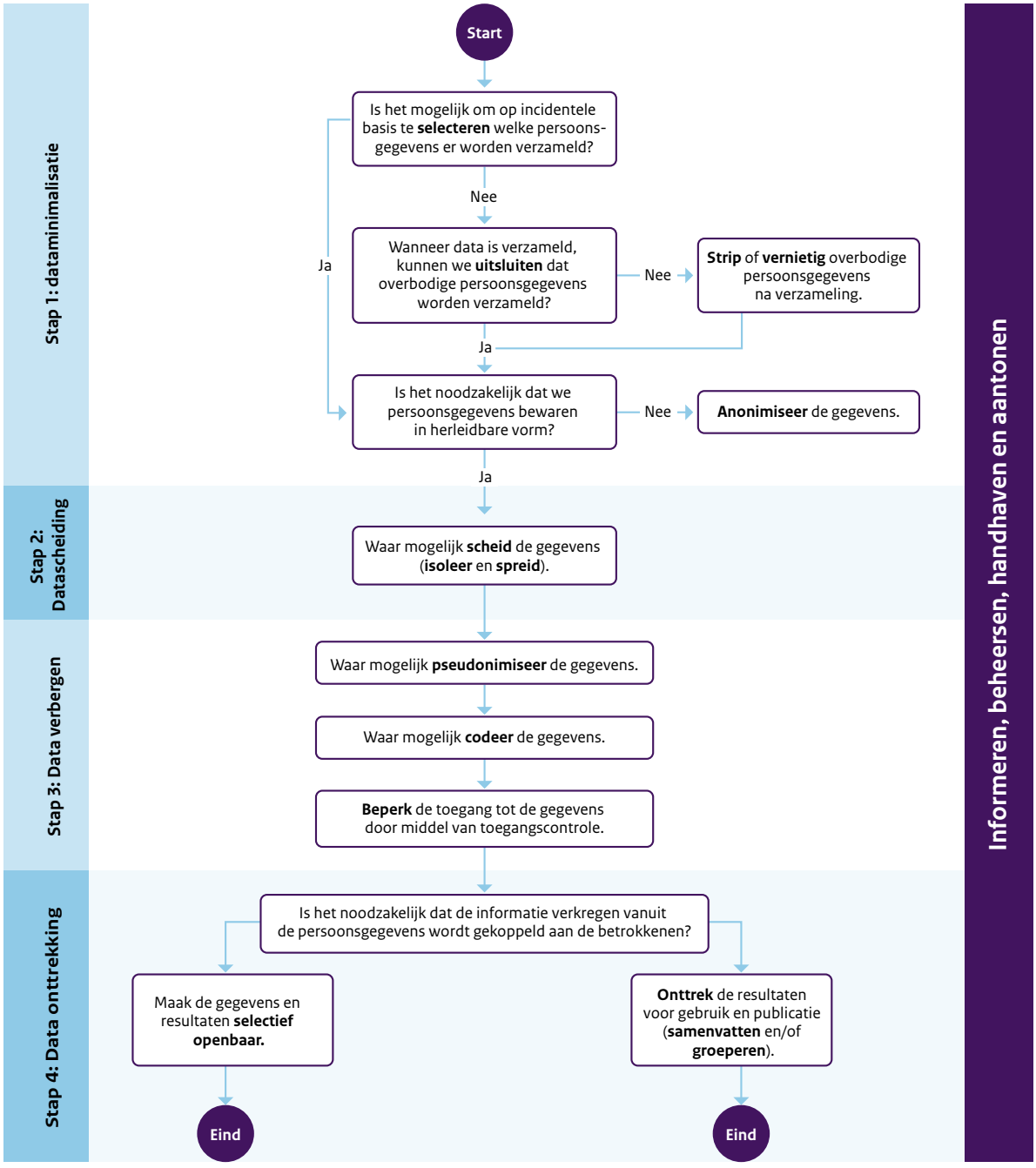
**Tabel 2.1.** PbD ontwerpstrategieën en tactieken.

| STRATEGIE | TECHNISCHE STAPPEN |
|---|---|
| **Data georiënteerd** | |
| Minimaliseer | Selecteer |
| | Sluit uit |
| | Verwijder |
| | Vernietig |
| Scheid | Isoleer |
| | Distribueer |
| Verberg | Beperk toegang |
| | Maak onbegrijpbaar |
| | Versleutel |
| | Verbreek link |
| | Meng |
| Abstraheer | Groepeer |
| | Vat samen, generaliseer |
| | Voeg ruis toe, verstoor |
| **Proces georiënteerd** | |
| Informeer | Informeer |
| | Leg uit |
| | Waarschuw |
| Geeft controle | Vraag |
| | Geef keuze |
| | Corrigeer |
| | Verwijder |
| Dwing af | Stel vast |
| | Dwing af |
| | Beheer |
| Toon aan | Leg vast |
| | Audit |
| | Rapporteer |

## 2.3. PbD beslisboom

De PbD ontwerpstrategieën moeten worden doorlopen wanneer persoonsgegevens (zullen) worden verwerkt, wanneer systemen, applicaties, processen, beleid en producten worden ontworpen. De volgende **beslisboom** (zie figuur 2.3) helpt in het meenemen van de genoemde ontwerpstrategieën. In deze beslisboom worden de woorden "waar mogelijk" gebruikt. Dit houdt geen verplichting in dat het ook moet. "Mogelijk" verwijst naar het resultaat van de zorgvuldig afgewogen maatregelen die wel of niet worden genomen. Bijvoorbeeld: als in een concreet geval gedegen is besloten dat er geen pseudonimisering wordt toegepast, is dat ook goed.

**Figuur 2.3.** PbD beslisboom.



Zie voor achtergrondinformatie over de noodzakelijkheid van de verwerking van persoonsgegevens paragraaf 6.2 van deze handleiding.

## 2.4. Verhouding PbD ontwerpstrategieën en privacybeginselen

De ontwerpstrategieën en de privacybeginselen voor een behoorlijke gegevensverwerking zoals neergelegd in de AVG houden sterk verband met elkaar. Door de vuistregels aan te houden bij de implementatie van de relevante ontwerpstrategieën, wordt tegelijkertijd deels invulling gegeven aan de privacybeginselen.

Zie voor achtergrondinformatie over de theoretische verhouding tussen PbD en de privacybeginselen uit de AVG paragrafen 4.2 en 6.1 van deze handleiding.

In tabel 2.2 hieronder komen deze twee elementen samen en wordt het verband gelegd tussen een strategie en het meest passende beginsel uit artikel 5 AVG bij die strategie. De tabel dient als volgt te worden opgevat (geïllustreerd als voorbeeld): als de strategie 'minimaliseer' wordt toegepast, draagt dat bij aan het beginsel van minimale gegevensverwerking uit artikel 5.

**Tabel 2.2.** Ontwerpstrategieën in verhouding tot de privacybeginselen voor gegevensverwerking.

| Strategie | Draagt bij aan beginsel artikel 5 AVG | Toelichting |
|---|---|---|
| **Data georiënteerd** | | |
| Minimaliseer | Minimale gegevensverwerking (Art. 5 lid 1 sub c AVG) | Wanneer in een processen wordt vastgelegd dat alleen persoonsgegevens x en y worden verwerkt, en geen andere persoonsgegevens omdat die andere persoonsgegevens niet écht nodig zijn voor het doel, wordt rekening gehouden met deze strategie en dit beginsel.<br><br>Voorbeelden:<br>• Wanneer het bijvoorbeeld in een webformulier alleen mogelijk is om persoonsgegevens x en y in te vullen en geen andere persoonsgegevens.<br>• Wanneer bijvoorbeeld in systemen extra persoonsgegevens buiten x en y automatisch worden gewist als deze per ongeluk wel worden verwerkt. |
| Scheid | Doelbinding (Art. 5 lid 1 sub b AVG) | Door persoonsgegevens in verschillende databases op te slaan, wordt het lastiger deze te combineren en daarmee voor andere doelen te gebruiken, waarmee rekening wordt gehouden met deze strategie en dit beginsel. |
| Verberg | Integriteit en vertrouwelijkheid (Art. 5 lid 1 sub c AVG) | Wanneer in autorisatiebeleid wordt vastgelegd welke medewerkers wel en geen toegang hebben tot persoonsgegevens, wordt rekening gehouden met deze strategie en dit beginsel. |

| Strategie | Draagt bij aan beginsel artikel 5 AVG | Toelichting |
|---|---|---|
| Onttrek | Minimale gegevensverwerking (Art. 5 lid 1 sub f AVG)<br><br>Opslagbeperking (Art. 5 lid 1 sub e AVG) | Wanneer het nodig is om iemands leeftijd te registreren, kan ook worden volstaan met het registreren van de leeftijd in plaats van de geboortedatum. In dat geval wordt rekening gehouden met deze strategie en dit beginsel. |
| **Proces georiënteerd** | | |
| Informeer | Rechtmatigheid, behoorlijkheid en transparantie (Art. 5 lid 1 sub a AVG) | Wanneer betrokkenen de privacyverklaring gemakkelijk kunnen vinden en hun privacy rechten kunnen uitoefenen, wordt rekening gehouden met deze strategie en dit beginsel.<br><br>Wanneer de privacyverklaring toegankelijk is voor personen met een visuele beperking, wordt rekening gehouden met deze strategie en dit beginsel. |
| Beheers | Rechtmatigheid, behoorlijkheid en transparantie (Art. 5 lid 1 sub a AVG)<br><br>Juistheid (Art. 5 lid 1 sub d AVG)<br><br>Opslagbeperking (Art. 5 lid 1 sub d AVG) | Wanneer aan betrokkenen, bijvoorbeeld door een privacy dashboard, de mogelijkheid wordt gegeven hun eigen persoonsgegevens aan te passen, wordt rekening gehouden met deze strategie en dit beginsel. |
| Handhaaf | Verantwoordingsplicht (Art. 5 lid 2 AVG) | Wanneer bij een nieuwe aankoop van een applicatie bij de leverancier wordt nagevraagd hoe deze leverancier concreet aan PbD voldoet, wordt rekening gehouden met deze strategie en dit beginsel.<br><br>Wanneer iedere nieuwe medewerker een training krijgt over de AVG en daarbij ook PbD wordt meegenomen, wordt rekening gehouden met deze strategie en dit beginsel. |
| Toon aan | Verantwoordingsplicht (Art. 5 lid 2 AVG) | Wanneer de genomen stappen en afwegingen i.v.m. PbD worden vastgelegd/gedocumenteerd, wordt rekening gehouden met deze strategie en dit beginsel.<br><br>Wanneer een DPIA wordt uitgevoerd, wordt rekening gehouden met deze strategie en dit beginsel.<br><br>Wanneer een privacy managementsysteem is opgezet, wordt rekening gehouden met deze strategie en dit beginsel. |

# 3. Inbedding PbD en best practices

Bij het toepassen van PbD kunnen de volgende drie stappen vanaf de eerste dag in het ontwerpproces worden onderscheiden:

**STAP 1.**
Identificeer en beoordeel risico's op basis van het voorgestelde ontwerp van het systeem of proces.

**STAP 2.**
Risicobeperkende maatregelen voorstellen en selecteren met behulp van ontwerpstrategiëen.

**STAP 3.**
Documenteer de genomen risicobeperkende maatregelen.

## 3.1. Stap 1: Risicobeoordeling

**Risicobeoordeling** is het identificeren en beoordelen van de risico's van een (voorgenomen) verwerkingsactiviteit. Realiseer je hierbij dat maatregelen nooit alle gevaren kunnen wegnemen. De context bepaalt wat je beschermt, tegen wie en hoe. Er moet een balans zijn tussen veiligheid, bruikbaarheid en kosten.

**Figuur 3.1.** Kwantificering risico.


| Impact | Kans |
|---|---|
| Wat is het negatieve effect – dat wil zeggen privacy schade - van een ongewenst/onbedoeld gevolg van een (voorgenomen) verwerkingsactiviteit? | Hoe groot is de kans dat die gevolgen zich daadwerkelijk voordoen? |
| **Aanvulling** | |
| Het is in de meeste vallen mogelijk om een objectief beeld van de impact te krijgen (aan de hand van scenario's en berekeningen) | Het kan lastig zijn om een objectief beeld van de kans te krijgen. |

Als er meer persoonsgegevens worden verwerkt dan noodzakelijk, heeft dat een grote impact op betrokken. Dit is de **impact/effect** van het risico. Dit alles leidt er namelijk toe dat betrokkenen minder vertrouwen hebben in de organisatie en het veel moeite zal gaan kosten om de gegevens op te ruimen. Dit zijn de **gevolgen** van het risico.

Risico's die zich kunnen voordoen in het kader van de verwerking van persoonsgegevens kunnen zich manifesteren in fysieke, materiële of immateriële schade.

In **bijlage C.** is een risicobeoordelingsmatrix met voorbeelden en nadere uitleg opgenomen. Deze bijlage kan behulpzaam zijn bij het inschatten van het risico.

### Welke maatregelen kunnen worden genomen om de risico's weg te nemen?

Waar uit de risicobeoordeling blijkt dat er risico's verbonden zijn aan de verwerking van persoonsgegevens, moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen implementeren om de privacy van betrokkenen te waarborgen. De PbD beslisboom (zie figuur 2.3) kan hierbij een behulpzaam middel vormen.

Zie voor meer uitleg over wat als "passende" technische en organisatorische maatregelen moeten worden beschouwd paragraaf 5.2 van deze handleiding.

In aanvulling op deze nadere uitleg geldt dat de mate waarin technische en organisatorische maatregelen als passend worden beschouwd afhangt van de geschatte schade aan de **vertrouwelijkheid**, **integriteit** en **beschikbaarheid** van informatie en systemen (zie tabel 3.1).

**Tabel 3.1.** Invulling passende maatregelen in verband met vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen.

| **Eis aan vertrouwelijkheid** | |
|---|---|
| Laag | Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. |
| Midden | Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. |
| Hoog | • verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;<br>• informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of<br>• aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of<br>• weerstand tegen statelijke actoren is noodzakelijk. |
| **Eis aan integriteit** | |
| Laag | Het verlies van integriteit kan leiden tot beperkte schade. |
| Midden | Het verlies van integriteit kan leiden tot forse schade. |
| Hoog | Ernstigere schade dan het bij "Midden" beschreven schadescenario. De integriteitseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken. . |

| Eis aan beschikbaarheid | |
|---|---|
| Laag | Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade. |
| Midden | Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade. |
| Hoog | Significant ernstigere schade dan het bij "Midden" beschreven schadescenario. De beschikbaarheidseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken. |

**Tip:** zoek in ieder geval bij het inventariseren van de mogelijke technische en organisatorische maatregelen ondersteuning bij een collega die zich bezighoudt met informatiebeveiliging en/of privacy en gegevensbescherming.

### Identificeer per maatregel:

**KOSTEN**
In grote lijnen geldt dat wanneer het risico klein of gemiddeld is, maar de kosten van een maategel heel hoog zijn, deze maatregel waarschijnlijk niet het meest passend is. Wanneer het risico hoog is en de kosten van de maatregel ook hoog, geldt dat deze maatregel waarschijnlijk toch toegepast moet worden.

| Voorbeelden | |
|---|---|
| **Risico klein of gemiddeld, kosten maatregel hoog** | **Risico hoog, kosten maatregel hoog** |
| Eens per maand wordt een lijst met namen van 20 medewerkers die meedoen aan een verdiepingssessie over PbD intern rondgemaild. | Eens per week wordt een lijst met namen en BSN-nummers van 10 burgers gedeeld die in verband worden gebracht met ondermijnende activiteiten in de gemeente waar zij wonen. |
| Omdat die lijst persoonsgegevens bevat, moet er gebruik worden gemaakt van veilig mailen. | Omdat die lijst persoonsgegevens bevat, moet er gebruik worden gemaakt van veilig mailen. |
| De (dure) licentie van veilig mailen laat voor de hele afdeling maar 25 mails per jaar toe. Collega's die ook vertrouwelijk willen emailen, lopen vaak tegen de lamp omdat er al 12 emails per jaar worden gebruikt voor het versturen van deze lijst. | De (dure) licentie van veilig mailen laat voor de hele afdeling maar 25 mails per maand toe. Collega's die ook vertrouwelijk willen emailen, lopen vaak tegen de lamp omdat er al 4 emails per maand worden gebruikt voor deze lijst. |
| → Het gebruik van de (dure) licentie van het veilig mailen is in dit geval niet een proportionele maatregel in verhouding tot het risico. | → Het gebruik van de (dure) licentie van het veilig mailen is in dit geval wel een proportionele maatregel in verhouding tot het risico. Als het lijstje namelijk lekt of wordt bekeken door een niet-geautoriseerd persoon, kan dit grote consequenties hebben voor de betrokkenen. |

**BRUIKBAARHEID**
In grote lijnen geldt dat wanneer het risico klein of gemiddeld is en de invoer van de maatregel leidt tot allerlei problemen in de uitvoering, dit waarschijnlijk niet de meest passende maatregel is. Wanneer het risico groot is en invoering van de maatregel leidt tot allerlei problemen in de uitvoering, dient de maatregel te worden aangepast waardoor de problemen in de uitvoering minder hoog worden.

**Voorbeelden**

**Risico klein of gemiddeld, maatregel heeft invloed op de bruikbaarheid**

Voor de dagelijkse werkzaamheden van X is het voor medewerkers van belang dat zij kunnen kijken hoe er in vergelijkbare zaken is geoordeeld door X en welke factoren daarbij een rol hebben gespeeld.

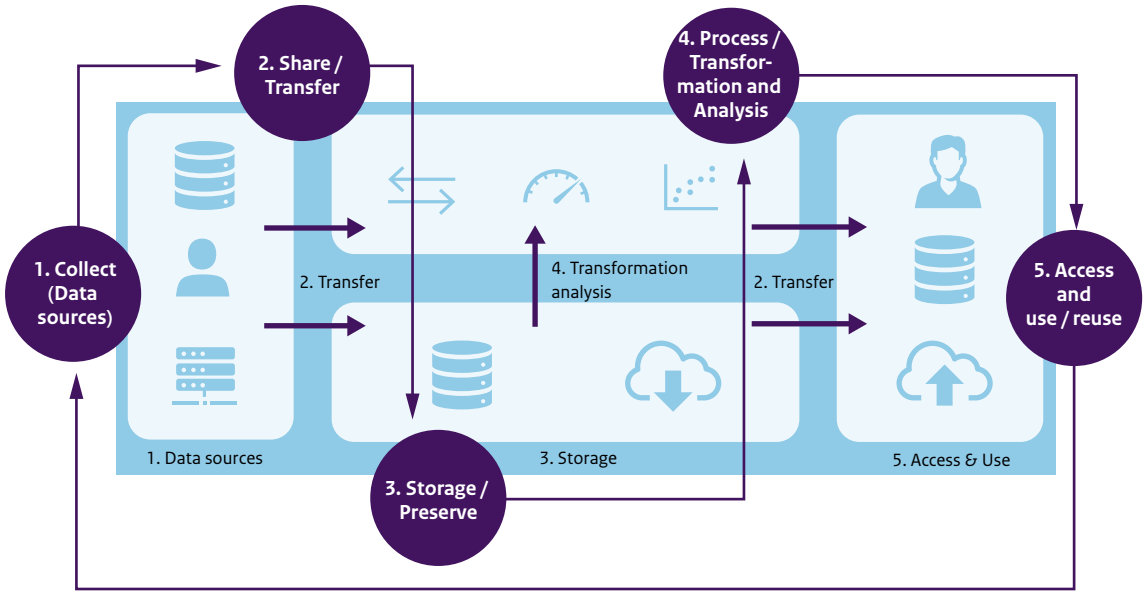
Omdat de dossiers persoonsgegevens bevatten, is besloten dat van de 100 betrokken medewerkers alleen Y nog toegang heeft tot de oude dossiers. De toegang voor de andere medewerkers is volledig afgesloten.

Y is vaak afwezig en 99 medewerkers moeten soms weken wachten op antwoord. Daarmee komen wettelijke beslistermijnen in gevaar.

Met een kleine aanpassing, namelijk dat de namen van de betrokkenen uit de oude dossiers worden afgeschermd en een technische aanpassing dat de 99 medewerkers oude stukken niet meer kunnen aanpassen, wordt het toch mogelijk voor 99 medewerkers om in de oude dossiers te kijken. Hiermee zijn de genomen maatregelen proportioneel in verhouding tot het geïdentificeerde risico voor X.

PbD beoogt een privacyvriendelijk ontwerp van systemen en processen en helpt daarmee privacy schade te voorkomen. Conceptueel spelen hierbij verschillende verwerkingsstromen (gegevens verzamelen, opslaan, transformeren/ gebruiken en toegankelijk maken) die meegenomen moeten worden (zie figuur 3.2).

**Figuur 3.2.** Componenten van gegevensverwerkingen binnen systemen en processen.




Informatiesystemen verzamelen gegevens van een externe gegevensbron (1), bijvoorbeeld uit databanken van derden, uit webformulieren, door sensoren worden verzameld, etc. Deze gegevens worden overgebracht (2) van de oorspronkelijke gegevensbron naar het informatiesysteem, bijvoorbeeld wanneer gegevens via een API van een derde partij worden verzameld en vervolgens via een beveiligde verbinding worden overgedragen. Zodra de gegevens zijn opgenomen, worden zij (tijdelijk) opgeslagen (3) in het informatiesysteem. Zodra de gegevens zijn opgeslagen, kunnen ze worden gebruikt voor de doeleinden waarvoor ze verzameld zijn (4); ofwel analyse (4), ofwel toegang en (her)gebruik (5), ofwel een combinatie. Gegevens uit het systeem kunnen ook worden doorgegeven (2) aan derden.

Hieronder volgt een tabel met aandachtspunten bij bovengenoemde componenten die bij de inrichting van systemen en processen moeten worden meegewogen (zie tabel 3.2).

**Tabel 3.2.** Relevante componenten voor de inrichting van systemen en processen.

| Component | Aandachtspunten |
|---|---|
| (1) Verzameling (databronnen) | • Mogen we de bronnen aansluiten?<br>• Kunnen we het inlezen van de gegevens controleren/beperken?<br>• Kunnen we de bronnen afkoppelen?<br>• Kunnen we de kwaliteit van de data controleren?<br>• Zijn de verbindingen met ons systeem beveiligd? |
| (2) Delen/ overbrengen | • Waarom delen we de data?<br>• Is de reden voor het delen van persoonsgegevens verenigbaar met het oorspronkelijke doel van de verwerking?<br>• Met wie delen we de data?<br>• Wie krijgen toegang tot de data?<br>• Kan het delen van data op een veilige manier met inachtneming van beveiligingsoverwegingen? |
| (3) Opslag | • Zijn de gegevens correct ingeladen?<br>• Hoe zijn de gegevens beveiligd?<br>• Worden de gegevens buiten de EU opgeslagen?<br>• Hoe is de toegang tot gegevens geregeld?<br>• Worden de gegevens door een derde opgeslagen (verwerker); zo ja, wat gebeurt daar dan mee? |
| (4) Verwerking/ analyse | • Welke transformaties ondergaan de data?<br>• Zijn deze verwerkingen/ analyses effectief?<br>• Zijn onze modellen accuraat? |
| (5) (Her)gebruik | • Voor welke doeleinden worden de data (her)gebruikt?<br>• Wie heeft toegang tot de data?<br>• Wie zijn ontvangers van onze data?<br>• Maken we persoonsgegevens openbaar? |

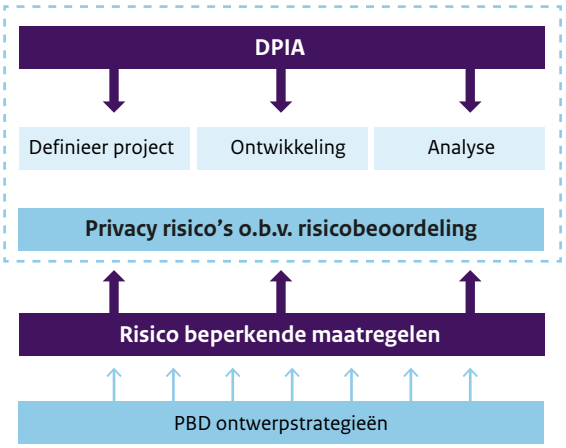
Naast het hiervoor genoemde, kan het uitvoeren van een **DPIA** bijdragen aan de vaststelling van de privacy risico's bij het verwerken van persoonsgegevens.[4]

**Let op:** op basis van de AVG is een DPIA in een aantal gevallen verplicht, bijvoorbeeld wanneer de verwerking een 'hoog risico' inhoudt. Er zijn verschillende checklists (Pre-DPIA's) die hierop sturen. De vragen in zulke checklist zoeken naar de verplichte gevallen waarin een DPIA moet worden uitgevoerd. PbD moet altijd worden toegepast, ook bij verwerkingen die een 'laag risico' inhouden. De te nemen PbD maatregelen zijn bij een laag-risico verwerking wellicht wel minder omvangrijk dan bij een hoog-risico verwerking. Stel dat uit de pre-DPIA als uitkomst komt dat er geen DPIA moet worden uitgevoerd, omdat de verwerking bijvoorbeeld niet hoog risico is, betekent dat dus niet dat je dan klaar bent met PbD. Ook in die gevallen moet er kritisch worden gekeken hoe PbD op de verwerking kan worden toegepast.

4 DPIA (artikel 35 AVG). Een verwerkingsverantwoordelijke moet voorafgaand aan een verwerkingsactiviteit een DPIA uitvoeren wanneer de betreffende verwerking waarschijnlijk een hoog risico met zich meebrengt voor de rechten en vrijheden van natuurlijke personen. Hierin voert de verwerkingsverantwoordelijke een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Bij het vaststellen van de noodzaak om een DPIA uit te voeren, spelen de volgende aspecten een bepalende rol: het gebruik van nieuwe technologieën en de aard, de omvang, de context en de doeleinden van de verwerkingsactiviteit(en).

Een DPIA is een instrument dat kan worden gebruikt voor het identificeren van privacyrisico's. Een DPIA kan ook behulpzaam zijn, om vanuit de PbD-ontwerpstrategieën, PbD effectiever toe te passen. (zie figuur 3.3).

**Figuur 3.3.** Uitvoering DPIA in verband met PbD ontwerpstrategieën.




Hoe de voorgestelde en geselecteerde passende technische en organisatorische maatregelen zich tot de PbD ontwerpstrategieën verhouden, wordt verder besproken in paragraaf 3.2.

## 3.2. Stap 2: Risicobeperkende maatregelen voorstellen en selecteren

Nadat de risicobeoordeling heeft plaatsgevonden is het van belang om **risicobeperkende maatregelen** voor te stellen en te selecteren om de geïdentificeerde privacy risico's te beperken.

Risicobeperkende maatregelen moeten toegepast in alle fasen van de levenscyclus van de verwerking, niet alleen aan het begin. De PbD beslisboom (zie figuur 2.3) biedt een weergave van de stappen die hierbij genomen moeten worden.

Onderstaande tabel biedt een weergave van de vragen die hierbij centraal staan:

**Tabel 3.3.** Relevante vragen bij de inventarisatie van risico beperkende maatregelen gedurende de fasen van de levenscyclus van de verwerking.

| Fase van de levenscyclus[5] | Relevante vragen | Relevante rollen (indicatie) |
|---|---|---|
| **Voorstel en definiëring verwerking** | Is het nodig dat persoonsgegevens verwerkt worden? | Systeem architect; PO |
| | Kan deze verwerking op basis van een grondslag in de AVG gerechtvaardigd worden? | PO, FG |
| | Is vernietiging of anonimisering persoonsgegevens direct na verwerking mogelijk? | Systeem architect; Solution architect |

5 Niet alle fases zoals in de tabel beschreven, doen zich voor bij ieder product, applicatie, dienst, etc. Het is dan ook van belang om eerst in kaart te brengen wat de levenscyclus in kaart te brengen.

| Fase van de levenscyclus[5] | Relevante vragen | Relevante rollen (indicatie) |
|---|---|---|
| **Informatieanalyse** | Welk niveau van bescherming is nodig om de geïdentificeerde risico's te beperkten en de ambities, zoals beschreven in het privacy beleid, te bereiken? | Systeem architect; Solution architect; PO; Functionaris beveiliging |
| | Welke verwerkingsprocessen maken gebruik van welke informatie, ofwel hoe ziet de gegevens-verwerking eruit? | Systeem architect |
| | Welke technische maatregelen zijn nodig naast organisatorische maatregelen en vullen de organisatorische maatregelen aan? | Systeem architect; Solution architect; Functionaris beveiliging; Chief Information Security Officer |
| | Zijn er al technische maatregelen gedefinieerd en geïmplementeerd om persoonsgegevens te beschermen? | Systeem architect; Solution architect; Beheerder(s); Chief Information Security Officer |
| **Ontwerp** | Welke gegevens worden verwerkt en op welke grond? | Systeem architect; PO |
| | Hoe lopen de gegevensstromen in het informatiesysteem? | Systeem architect |
| | Kan de inhoudelijke kwaliteit van de gegevens worden gecontroleerd en aangepast? | Systeem architect; Solution architect; Product managers/ developers; PO; Functionaris beveiliging |
| | Hoe worden de betrokkenen ingelicht? | PO; FG |
| | Wat is het gegevensmodel voor iedere gegevensstroom in het verwerkingsproces van verzamelen, opslaan, bewaren tot aan vernietigen? | Systeem architect; Solution architect |
| | Welke koppelingen met andere systemen en instanties zijn in ketenverband aanwezig en welke gronden zijn daarvoor? | Systeem architect; PO; Chief Information Security Officer |
| | Welke voorzieningen zijn er om de juistheid en nauwkeurigheid van persoonsgegevens te bewaken? | Beheerders; PO; FG |
| | Welke voorzieningen zijn er zodat de betrokkene persoonsgegevens kan laten corrigeren of overgedragen te krijgen? | Beheerders; PO; FG |
| | Leveren de privacymaatregelen de juiste informatie ten behoeve van toezicht en toegang? | PO; FG; Functionaris beveiliging |

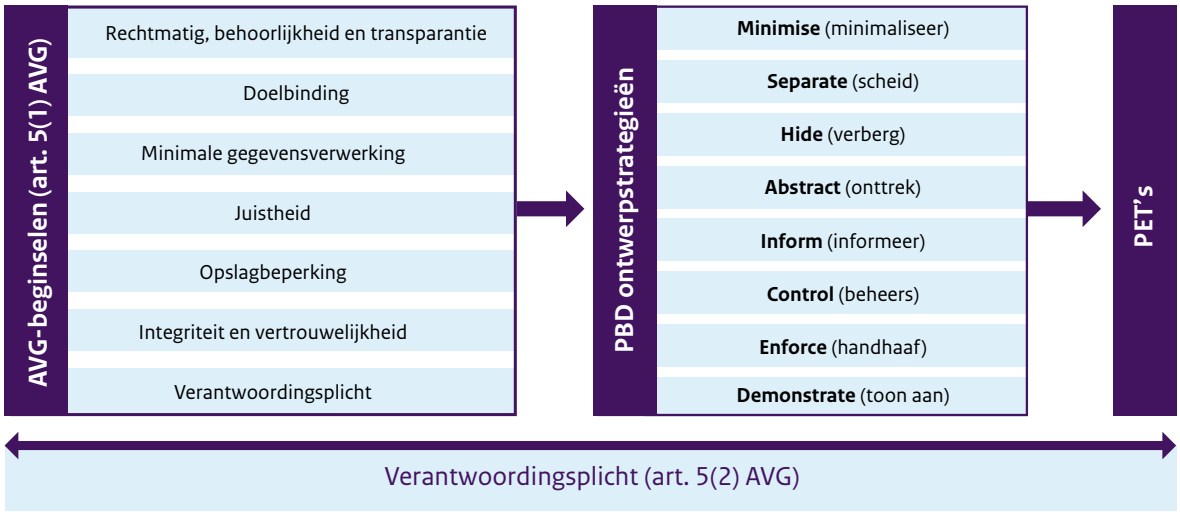
| Fase van de levenscyclus[5] | Relevante vragen | Relevante rollen (indicatie) |
|---|---|---|
| | Is een rapportage in geval van een datalek mogelijk? | PO; FG; Functionaris beveiliging |
| | Zijn de verantwoordelijkheden duidelijk? | Bestuur/ directie |
| | Welke beveiligingseisen worden aan de technische maatregelen gesteld? | Functionaris beveiliging; Chief Information Security Officer |
| | Hoe worden de technische maatregelen geïntegreerd in het volledige technisch ontwerp van het informatiesysteem? | Systeem architect; Solution architect |
| | Zijn de verantwoordelijkheden duidelijk? | Bestuur/ directie |
| **Ontwikkeling** | Moet de gekozen technische maatregel zelf worden ontwikkeld of zijn er standaardoplossingen beschikbaar? | Systeem architect; Solution architect |
| **Testen** | Functioneren de technische en organisatorische maatregelen op een juiste wijze als onderdeel van de gehele informatieverwerking? | Solution architect; Product managers/ developers; Functionaris beveiliging |
| | Voldoen de geïmplementeerde technische maatregelen aan de eisen voor gebruikersvriendelijkheid? | Testers/ user acceptance |
| | Hoe vindt anonimiseren plaats (en hoe is het meegenomen in het ontwerp) of hoe vindt op een andere wijze de bescherming van de persoonsgegevens plaats? | Systeem architect; Solution architect |
| | Zijn de verantwoordelijkheden duidelijk? | Bestuur/ directie |
| **Implementatie** | Verandert de werkwijze voor gebruikers door de toepassing van de technische maatregelen en hoe worden gebruikers hierover ingelicht? | Testers/ user acceptance |
| | Moeten betrokkenen, waarvan de persoonsgegevens worden verwerkt, worden ingelicht? | PO; FG |
| | Moeten beheerders en gebruikers getraind worden in de toepassing van de technische maatregelen? | Functionaris beveiliging |
| | Zijn de verantwoordelijkheden duidelijk? | Bestuur/ directie |
| **Beheer en onderhoud** | Welke specifieke privacy-beheeractiviteiten moeten worden uitgevoerd in aanvulling op de reguliere beheeractiviteiten? | Beheerders; PO; FG |
| | Zijn de verantwoordelijkheden duidelijk? | Bestuur/ directie |

| Fase van de levenscyclus[5] | Relevante vragen | Relevante rollen (indicatie) |
|---|---|---|
| **Evaluatie** | Zijn de privacy maatregelen effectief? | PO; FG |
| | Is een audit of een certificering van het informatiesysteem gewenst? | POs; functionaris beveiliging; Chief Information Security Officer |
| | Wat zijn de gebruikers-en beheerderservaringen? | Testers/ user acceptance |

Zie voor achtergrondinformatie over de relevante rollen in het kader van de praktische inbedding van PbD hoofdstuk 7 van deze handleiding.

Om de beginselen die in hoofdstuk 4 zijn besproken te vertalen naar concrete functionele vereisten, zijn de PbD ontwerpstrategieën behulpzaam. Aan deze ontwerpstrategieën kunnen op hun beurt in de praktijk invulling worden gegeven via PET's (zie figuur 3.4).

**Figuur 3.4.** Implementatie van PbD via AVG-beginselen, PbD ontwerpstrategieën en PET's.




In de praktische vertaalslag van AVG-beginselen naar PbD ontwerpstrategieën en uiteindelijk naar PET's is het van belang voor alle relevante partijen om inzicht te krijgen in de technische en organisatorische maatregelen die zij kunnen nemen om praktische invulling te geven aan PbD in het ontwerp van systemen, applicaties, processen, beleid en producten waarbij persoonsgegevens een rol spelen.

Zie voor achtergrondinformatie over de verhouding tussen PbD, ontwerpstrategieën en PET's paragraaf 4.3 van deze handleiding.

### 3.2.1. Toolkit implementatie PbD middels technische en organisatorische maatregelen

In deze handleiding zijn deze technische en organisatorische maatregelen onderverdeeld in **technische en organisatorische toolkits**.[6] Welke toolkit "passend" is, is afhankelijk van de specifieke situatie. De toolkits houden verband met de PbD ontwerpstrategieën en privacybeginselen en omvatten:

6 Deze toolkits kunnen worden aangevuld op basis van de laatste stand van de techniek en nieuwe *best practices* of beleid.

**Tabel 3.4.** Toolkit implementatie PbD middels technische en organisatorische maatregelen.

<table>
<tr><th colspan="4">TECHNISCHE EN ORGANISATORISCHE TOOKITS TER IMPLEMENTATIE VAN PBD</th></tr>
<tr><td colspan="4">Data georiënteerd</td></tr>
<tr><td colspan="2">TOOLKIT 1</td><td colspan="2">TOOLKIT 2</td></tr>
<tr><td colspan="2">MINIMALSEER</td><td colspan="2">SCHEID</td></tr>
<tr><td>Selecteer<br>Sluit uit<br>Verwijder<br>Vernietig</td><td>VOORBEELDEN<br>/ Select before you collect (whitelists)<br>/ Blacklists<br>/ Strip or destroy<br>/ Anonimisering</td><td>Isoleer<br>Distribueer</td><td>VOORBEELDEN<br>/ Peer-to-peer<br>/ Doe zoveel mogelijk in de apparatuur van de eindgebruiker<br>/ Classificatie bronnen/ data & labeling<br>/ Data lineage</td></tr>
<tr><td></td><td>PET’S (VOORBEELDEN)<br>Anonymization techniques (data altering)<br>Differential Privacy (data altering)<br>Secure Multi-Party Computation (computation altering)</td><td></td><td>PET’S (VOORBEELDEN)<br>Pseudonymization techniques (data altering)<br>Federated Learning/Analytics (computation altering)<br>Trusted Execution environments (data shielding)<br>Secure Multi-Party Computation (computation altering), including private-set intersection</td></tr>
<tr><td colspan="2">Minimale gegevensverwerking (art. 5 lid 1 sub c AVG)</td><td colspan="2">Doelbinding (art. 5 lid 1 sub b AVG)</td></tr>
<tr><td colspan="2">TOOLKIT 3</td><td colspan="2">TOOLKIT 4</td></tr>
<tr><td colspan="2">ABSTRAHEER</td><td colspan="2">BESCHERM/ MAAK ONHERLEIDBAAR</td></tr>
<tr><td>Groepeer<br>Vat samen/ generaliseer</td><td>VOORBEELDEN<br>/ Registreer leeftijd i.p.v. geboortedatum<br>/ Verzamel het energieverbruik in een wijk i.p.v. per huishouden<br>/ Attribuut gebaseerde credentials</td><td>Beperk toegang<br>Versleutel<br>Verbreek link<br>Meng<br>Maak onbegrijpbaar</td><td>VOORBEELDEN<br>/ Mix netwerken<br>/ Pseudonimiseren<br>/ Differential privacy<br>/ Access control (autorisaties)<br>/ Just-in-Time Privileged Access Management</td></tr>
<tr><td></td><td>PET’S<br>Anonymization techniques (data altering)<br>Differential Privacy (data altering)</td><td></td><td>PET’S<br>Encryption techniques such as zero knowledge proofs (data shielding)<br>Trusted Execution Environments (data shielding)<br>Homomorphic Encryption (data shielding)</td></tr>
</table>

| TECHNISCHE EN ORGANISATORISCHE TOOKITS TER IMPLEMENTATIE VAN PBD | |
|---|---|
| Minimale gegevensverwerking (art. 5 lid 1 sub c AVG); Opslagbeperking (art. 5 lid 1 sub e AVG) | Integriteit en vertrouwelijkheid (art. 5 lid 1 sub f AVG) |

**Proces georiënteerd**

| TOOLKIT 5 | | TOOLKIT 6 | |
|---|---|---|---|
| INFORMEER | | GEEF CONTROLE | |
| Groepeer<br>Vat samen/ generaliseer | **VOORBEELDEN**<br>/ Leesbare privacy policy<br>/ Privacy icons<br>/ Algoritmische transparantie | Vraag toestemming<br>Geef keuze<br>Corrigeer<br>Verwijder | **VOORBEELDEN**<br>/ Opt-in<br>/ Recht om vergeten te worden |
| | **PET'S (VOORBEELDEN)**<br>Cryptographic Techniques (data shielding) (end to end user authentication) | | **PET'S (VOORBEELDEN)**<br>Cryptographic Techniques (data shielding) (end to end user authentication) |
| Rechtmatigheid, behoorlijkheid en transparantie (art. 5 lid 1 sub a AVG) | | Rechtmatigheid, behoorlijkheid en transparantie (art. 5 lid 1 sub a AVG); Juistheid (art. 5 lid 1 sub d AVG); Opslagbeperking (art. 5 lid 1 sub e AVG) | |
| **TOOLKIT 7** | | **TOOLKIT 8** | |
| DWING AF | | TOON AAN | |
| Stel vast<br>Beheer<br>Dwing af | **VOORBEELDEN**<br>/ Privacy policy<br>/ Beleg verantwoordelijkheden<br>/ Controleer het beleid, ende implementatie daarvan, regelmatig, en pas waar nodig aan<br>/ Neem noodzakelijke technische en organisatorische maatregelen | Leg vast<br>Audit<br>Rapporteer | **VOORBEELDEN**<br>/ Privacy management systeem (a la ISO 27001 security management)<br>/ Certificering<br>/ DPIA |
| | **PET'S (VOORBEELDEN)**<br>N.v.t. | | **PET'S (VOORBEELDEN)**<br>N.v.t. |
| Verantwoordingsplicht (art. 5 lid 2 AVG) | | Verantwoordingsplicht (art. 5 lid 2 AVG) | |

Hierna wordt per toolkit ingezoomd op de mogelijk acties die kunnen ondersteunen bij het implementeren van technische en organisatorische maatregelen.

## TOOLKIT 1 - MINIMALISEER

| TOOLKIT 1 | | | |
|---|---|---|---|
| **MINIMALISEER** | | | |
| **Selecteer** | **Sluit uit** | **Verwijder** | **Vernietig** |
| Bepaal of het mogelijk is gegevens per geval te verzamelen /dat de gegevensverzameling niet-incidenteel is. Als de verzameling niet incidenteel is, bepaal dan vóór de verzameling welke persoonsgegevens mogen worden verzameld (whitelists). | Als het niet mogelijk is alleen de noodzakelijke persoonsgegevens te selecteren en/of te verzamelen, bepaal dan of het mogelijk is persoonsgegevens van verzameling uit te sluiten (blacklists). Houd hierbij in het bijzonder rekening met gevoelige en bijzondere categorieën persoonsgegevens. | Als het niet mogelijk is persoonsgegevens te selecteren of van verzameling uit te sluiten, strip of vernietig de persoonsgegevens dan na verzameling.<br>**Strippen**: het verwijderen van onnodige (meta)gegevensvelden uit een gebruikersrecord of gegevensverzameling.<br>**Vernietigen**: het volledig verwijderen van persoonsgegevens uit een dataset. | |
| **Voorgestelde stappen gedurende de levenscyclus** | | | |
| • De hoeveelheid persoonsgegevens die wordt verzameld<br>- beperk waar het mogelijk is de soorten, categorieën en detailniveau van persoonsgegevens die worden verzameld. Dit geldt voor alle diensten en verwerkingsactiviteiten.<br>- Pas verschillende data minimaliserende technieken toe zoals de-identification technieken, differential privacy en secure multi-party computation.<br>- Beperk de mogelijke selecties om niet-noodzakelijke persoonsgegevens uit te sluiten bij het importeren van persoonsgegevens vanuit externe bronnen.<br>• De mate waarin zij worden verwerkt<br>- verwerk alleen persoonsgegevens die nodig zijn (*need to have*), niet de persoonsgegevens die misschien handig zijn (*nice to have*).<br>• De termijn waarvoor zij worden opgeslagen<br>- Verwijder (deel)gegevens die niet langer nodig zijn. Bepaal van tevoren hoe lang gegevens nodig zijn, en zorg dat ze automatisch na die tijd verwijderd worden.<br>- Stel bewaartermijnen vast. Stel procedures vast voor archiveren en opschonen (inclusief email en werkbestanden).<br>• De toegankelijkheid ervan<br>- Beperk de mogelijkheden om persoonsgegevens te kopiëren, printen, exporteren of te delen.<br>- Beperk en minimaliseer de blootstelling van onnodige functionaliteit en persoonsgegevens in de gebruikers-interface.<br>• Ontwerp de informatiesystemen op een wijze die gegevensuitwisseling via email en het gebruik van werkbestanden op netwerkschijven overbodig maakt.<br>• Controleer de DPIA en pas deze waar nodig aan. | | | |
| VOORBEELD | | | |
| Uitvoeringsorganisatie X is wettelijk verplicht een administratie bij te houden. In de wet staat dat voor die administratie gezichtsopnames en vingerafdrukken moeten worden opgenomen. X beperkt zich bij het verzamelen van deze gegevens tot gezichtsopnames en vingerafdrukken, en verwerkt niet ook de stem van de betrokkenen of andere fysieke kenmerken, voor het geval dat handig zou kunnen zijn in de toekomst.<br><br>Het systeem van X is bovendien zo ingericht dat er maar twee velden zijn waar gegevens kunnen worden ingevoerd; het gezichtsopname veld en het vingerafdruk veld. Deze gegevens kunnen niet worden geëxporteerd of lokaal worden opgeslagen door medewerkers van X.<br><br>Nadat de gezichtsopname en vingerafdrukken niet meer nodig zijn voor de administratie, zorgt X ervoor dat deze gegevens met inachtneming van de juiste bewaartermijnen, worden verwijderd. | | | |

## TOOLKIT 2 – SCHEID

| TOOLKIT 2 | |
|---|---|
| **SCHEID** | |
| **Isoleer** | **Distribueer** |
| Verwerk persoonsgegevens onafhankelijk, waardoor het moeilijker wordt om persoons-gegevens met elkaar te verbinden en correlaties tussen gegevenssets te leggen. | Verdeel de verwerking en opslag van persoons-gegevens, waardoor de single points of failure worden verminderd en aanvallers meer toegang tot het systeem nodig hebben om gegevens te verbinden en te correleren. |
| **Voorgestelde stappen gedurende de levenscyclus** | |
| Verzamel of verwerk persoonsgegevens in verschillende, logisch gescheiden, databases of systemen.<br>Distribueer de verwerking over verschillende fysieke locaties.<br>Beperk gegevensuitwisseling met organisaties/ teams die een andere taak uitvoeren.<br>Sla reguliere en gevoelige persoonsgegevens apart op.<br>Scheid tabellen in databases en bijbehorende wijs toegangsrechten tot tabellen en gebieden toe op basis van noodzaak.<br>Bemoeilijk de koppeling van gegevens aan elkaar, bijvoorbeeld het koppelen van rijen in tabellen binnen een database.<br>Zorg ervoor dat de gegevensverwerkingen op basis van verschillende doelen gescheiden plaatsvinden, met name naarmate de gevoeligheid van de data toeneemt en de doelen voor verwerking minder samenhangen.<br>Beperk de centrale opslag van persoonsgegevens tot een minimum.<br>Pas waar mogelijk verschillende technieken toe zoals federated learning/ analytics, trusted execution, secure multi-party computation, synthetic data, classificatie van bronnen/data en labeling, en data lineage. | |
| VOORBEELD | |
| Organisatie Y wil in kaart brengen hoeveel personen zich in een bepaalde stad identificeren met het gender non-binair door middel van een enquête. Respondenten kunnen meedoen op basis van de rechtsgrond uitdrukkelijke toestemming. In de enquête wordt onder meer gevraagd met welk gender de respondent zich identificeert en hoe veilig die persoon zich voelt om het gender waar die persoon zich mee identificeert, openlijk te communiceren. Uit die antwoorden zullen door organisatie Y algemene trends worden afgeleid. Om de enquête in te vullen moet iedere respondent een naam en e-mailadres invullen.<br>Organisatie Y slaat de contactgegevens (naam en e-mailadres) gescheiden van de antwoorden op de enquête. Wanneer iemand zich namelijk ongeoorloofd toegang verschaft tot de database met antwoorden, is het voor die persoon onmogelijk om te zien welke individu precies welk antwoord heeft gegeven. | |

## TOOLKIT 3 - ABSTRAHEER

| TOOLKIT 3 | |
|---|---|
| **ABSTRAHEER** | |
| **Groepeer** | **Vat samen/ generaliseer** |
| Gebruik en publiceren informatie op groepsniveau in plaats van op individueel niveau (bv. “werknemers” in plaats van “werknemer 1, 2 & 3”). | Vat de resultaten samen en verwijder de details in de gegevens op individueel niveau die tot de resultaten hebben geleid. |
| **Voorgestelde stappen gedurende de levenscyclus** | |
| Aggregeer informatie over categorieën personen in plaats van ieder individu en stel een groepsprofiel op.<br><br>Weergeef persoonsgegevens op basis van de relevante rol en de daaraan gekoppelde autorisaties op een ander aggregatieniveau.<br><br>Vat gedetailleerde informatie samen in meer algemene gegevens. Registreer bijvoorbeeld een leeftijds-categorie in plaats van een geboortedatum, of een woonplaats in plaats van het precieze adres.<br><br>Gebruik niet de precieze waarde van een gegeven. Gebruik een benadering van de waarde, of pas de waarde aan met een kleine hoeveelheid ruis.<br><br>Verwijder informatie wanneer deze onnodig zijn voor het beoogde doel.<br><br>Pas verschillende technieken toe zoals *de-identification techniques*, *differential privacy* en *federated learning*. | |
| VOORBEELD | |
| Organisatie X biedt abonnementen aan met verschillende tarieven. Zo geldt voor personen tussen 0-17 een gereduceerd tarief, tussen 18-64 het reguliere tarief en voor personen boven de 65 een sterk gereduceerd tarief.<br><br>X verwerkt alleen het geboortejaar van de klant en niet de precieze geboortedatum. Dit scheelt ook een hoop administratie. X heeft ook een oplossing bedacht voor het lopende jaar; als een specifiek geboortejaar in 2023 aanleiding geeft tot korting, wordt de korting ter voordeel van de klant toegepast op het moment dat de klant zich aanmeldt.<br><br>Een VOG wordt aangevraagd voor een specifiek screeningsprofiel. Alleen de voor het screeningsprofiel relevante onderdelen worden getoond. | |

## TOOLKIT 4 – BESCHERM/ MAAK ONHERLEIDBAAR

| TOOLKIT 4 | | | | |
|---|---|---|---|---|
| **BESCHERM/ MAAK ONHERLEIDBAAR** | | | | |
| **Beperk toegang** | **Versleutel** | **Verbreek link** | **Meng** | **Maak onbegrijpbaar** |
| Beperk toegang tot persoonsgegevens tot die rollen die toegang nodig hebben tot de persoonsgegevens door access control mechanismen (authenticatie en autorisatie) toe te passen. | Beveilig persoons-gegevens (zowel op het netwerk als bij opslag). | Verbreek de link tussen personen en gegevens. | Maak data onherleidbaar, bijvoorbeeld door deze te mixen of te anonimiseren. | Hash persoons-gegevens om er pseudoniemen van te maken. |
| **Voorgestelde stappen gedurende de levenscyclus** | | | | |
| Beperk toegang tot persoonsgegevens.<br>Zorg dat de informatiebeveiliging op orde is.<br>Stel strikte maatregelen voor toegangscontrole op en geef personen alleen toegang tot persoons-gegevens die ze strikt gesproken nodig hebben en bij voorkeur alleen op het moment dat ze dit nodig hebben (‘*need to know*’).<br>Segmenteer de gegevens in dossiers, zodat medewerkers toegang kan worden gegeven tot alleen die gegevens die ze nodig hebben voor hun werk.<br>In geval van hergebruik van data: verwijder de context en/of mix de data met willekeurige andere gegevens.<br>Maak data onbegrijpbaar voor derden door deze te versleutelen zodat ze onleesbaar worden zonder de sleutel. Hash persoonsgegevens, bijvoorbeeld om er pseudoniemen van te maken.<br>Gebruik met name encryptie wanneer gegevens moeten worden overgedragen naar ongecontroleerde gebieden of netwerken.<br>Vermijd onnodige blootstellingen aan communicatiepatronen en verbindingen (o.a. API’s, feeds, gateways, aanmeldingsinterfaces, enz.)<br>Voer bij het ontwerp van softwarebedreigingsmodellen een “attach surface analysis” uit.<br>Pas verschillende technieken toe zoals encryption, trusted execution environments, homomorphic encryption en synthetic data. | | | | |
| VOORBEELD | | | | |
| Organisatie Y moet een database bijhouden met strafbaar foto en video materiaal. Het materiaal wordt geencrypt. Alleen specifieke casemanagers krijgen de sleutel om het materiaal te kunnen decrypten. | | | | |

## TOOLKIT 5 – INFORMEER

| TOOLKIT 5 | | |
|---|---|---|
| **INFORMEER** | | |
| **Informeer** | **Leg uit** | **Waarschuw** |
| Informeer de betrokkene uitgebreid over de verwerking van persoonsgegevens, bijvoorbeeld via een privacyverklaring. | Verstrek deze informatie in een duidelijk en begrijpelijk formaat. Maak privacyverklaringen en andere vormen van informatie-verstrekking gemakkelijk te navigeren, te lezen en te begrijpen, door bijvoorbeeld gebruik te maken van gelaagde privacyverklaringen, iconen en infographics. | Waarschuw de betrokkenen wanneer wijzigingen of aanvullende verwerkingen (bv. via pop-upberichten) zich voordoen. |
| **Voorgestelde stappen gedurende de levenscyclus** | | |
| Geef de betrokkene toegang tot een uitleg waarom (doel en grondslag) de persoonsgegevens worden gevraagd. | | |
| Geef de betrokkene toegang tot een uitleg op welke manier de persoonsgegevens worden verwerkt. | | |
| Geef de betrokkene toegang tot de informatie over hoelang de persoonsgegevens bewaard blijven. | | |
| Stel vast op welke manier de betrokkene geïnformeerd zal worden over de verwerking? | | |

## TOOLKIT 6 – GEEF CONTROLE

| TOOLKIT 6 | | | |
|---|---|---|---|
| **GEEF CONTROLE** | | | |
| **Vraag toestemming** | **Geef keuze** | **Corigeer** | **Verwijder** |
| Wanneer de rechtsgrondslag voor gegevensverwerking toestemming van de betrokkene is, moet de betrokkene instrumenten en procedures ter beschikking worden gesteld waarmee hij ondubbelzinnig zijn toestemming kan geven.[7] | Biedt de betrokkene een zinvolle keuze om de verwerking van persoonsgegevens te beperken. Vermijd algemene strategieën en *take-it-or-late it*-opties. | Respecteer het recht van de betrokkenen om persoonsgegevens bij te werken of te corrigeren, bij voorkeur via een gebruikersagentschap (bv. Privacyportalen). | Respecteer de rechten van de betrokkenen om persoonsgegevens te verwijderen of de verwerking van persoonsgegevens te beperken, bij voorkeur via een gebruikersagentschap (bv. privacyportalen). |
| **Voorgestelde stappen gedurende de levenscyclus** | | | |
| Geef een daartoe bevoegde medewerker de mogelijkheid om de persoonsgegevens van een betrokkene op te vragen.<br>Stel de betrokkene in staat om zijn/haar rechten uit te oefenen.<br>Geef de betrokkene de mogelijkheid zijn/haar persoonsgegevens te raadplegen.<br>Geef de betrokkene de mogelijkheid om zijn/haar persoonsgegevens te (laten) wijzigen.<br>Geef betrokkenen de beschikking over een persoonlijk privacy dashboard met het oog op informatie, communicatie en uitoefening rechten. | | | |
| VOORBEELD | | | |
| Organisatie X vraagt burgers mee te doen aan onderzoeken via online vragenlijsten die via een app worden aangeboden. Burger A. heeft enkele van deze vragenlijsten ingevuld, maar merkt niet meer mee te willen doen. Via het privacy dashboard in de app kan burger A. direct een verzoek indienen tot verwijdering van alle persoonsgegevens. Dit verzoek wordt door organisatie X zo veel mogelijk automatisch uitgevoerd. Binnen enkele dagen ontvangt burger A. een automatisch genereerde bevestiging dat alle persoonsgegevens zijn verwijderd. In dit geval heeft organisatie X geen reden om bepaalde categorieën van persoonsgegevens van burger A. langer te bewaren. | | | |

7 De toestemmingsvereisten zijn in artikel 7 van de AVG opgenomen, zie https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf. Zie ook paragraaf 4.3.3. van de Handleiding AVG en UAVG (2023).

### TOOLKIT 7 – DWING AF

| TOOLKIT 7 | | |
|---|---|---|
| **DWING AF** | | |
| **Stel vast** | **Beheer** | **Dwing af** |
| Beoordeel risico's en tref risicobeperkende maatregelen voor de toepassing, dienst of het product dat wordt ontworpen. | Houd rekening met privacy en gegevensbescherming bij het aanbrengen van wijzigingen in de toepassing, de dienst of het product (gegevensbescherming tijdens de volledige levenscyclus). | Leef de regels en het beleid in verband met de toepassing van voornoemde maatregelen na. |
| **Voorgestelde stappen gedurende de levenscyclus** | | |
| Stel procedures en werkinstructies op.<br>Richt werkprocessen zo in dat kan worden gewerkt vanuit goed beveiligde dossiersystemen.<br>Borg de integriteit van de gegevens.<br>Leg afspraken met derden schriftelijk vast: borg een structureel veilige wijze van gegevensoverdracht. Let wel, dat ook moet worden nagedacht over het maken van afspraken tussen overheidsorganisaties onderling in de keten, met niet-overheidsorganisaties en in het geval van gezamenlijke verwerkingsverantwoordelijken.<br>Configureer logging en richt monitoring in.<br>Laat periodiek een audit of zelfevaluatie uitvoeren op onder meer: procedures en werkinstructies, autorisatiematrix en autorisaties en logging en monitoring. | | |

### TOOLKIT 8 – TOON AAN

| TOOLKIT 8 | | |
|---|---|---|
| **TOON AAN** | | |
| **Leg vast** | **Audit** | **Rapporteer** |
| Traceer elke verwerking van gegevens, zonder persoonsgegevens te onthullen, om aan te tonen dat de handelingen conform zijn (onweerlegbaarheid) en om het opsporen van niet-naleving (bv. ongeoorloofde toegang) mogelijk te maken. | Controleer systeemactiviteiten om risico's te beoordelen. Maak *audit trails* mogelijk voor de FG en de interne audit. | Analyseer en rapporteer periodiek om verbeteringen in de bescherming van persoonsgegevens te evalueren. |
| **Voorgestelde stappen gedurende de levenscyclus** | | |
| Actualiseer het verwerkingsregister.<br>Voer voor verwerkingen die een hoog risico inhouden voor de privacy van betrokkenen een DPIA uit.<br>Stel een toezichtsplan op, met het oog op controle en rapportage.<br>Breng per verwerker in kaart op welke onderwerpen gedurende de looptijd van de overeenkomst controles moeten worden uitgevoerd, en op welke wijze deze plaats zullen vinden. Werk volgens een *Plan-Do-Check-Act* (hierna: "PDCA") cyclus.<br>Rapporteer periodiek. | | |

### 3.2.2. Best practices

Naast de inbedding van PbD middels bovenstaande toolboxen voor technische organisatorische maatregelen, bieden onderstaande *best practices* ook aanvullende ondersteuning bij de implementatie van PbD. Deze lijst is niet uitputtend en kan worden aangevuld met nieuwe *best practices*.

Leeswijzer: de *best practices* zijn hierna gecategoriseerd aan de hand van een focuspunt en gekoppeld, waar mogelijk, aan de relevante fase in de levenscyclus. Voor de relevante fasen zijn 4 fasen aangehouden, zoals hieronder blijkt:

| Fase nr. | Fase beschrijving | Opmaak |
|---|---|---|
| 1 | Ontwerp | Voorstel en definiëring verwerking<br>Informatieanalyse<br>Ontwerp |
| 2 | Implementatie | Ontwikkeling<br>Testen<br>Implementatie |
| 3 | Uitvoering | Beheer en onderhoud<br>Evalueren |
| 4 | Afbouwen | N.v.t.[8] |

#### Het inrichten van de organisatorische infrastructuur

| | |
|---|---|
| Stel een PO aan. | 1 |
| Stel privacy ambassadeurs aan die de privacy op de werkvloer waarborgen en terugkoppelen aan de PO(s) over privacyvraagstukken. | 1 |
| Zorg ervoor dat alle relevante interne stakeholders – en identificeer deze - vroegtijdig bij de inrichting van het proces betrokken worden. | 1 2 |
| Zorg ervoor dat bij de inrichting van nieuwe processen een gesprek plaatsvindt met de PO(s). Doe dit op tijd. | 1 2 |
| Zorg ervoor dat de PO door iedereen binnen de organisatie gevonden en benaderd kan worden. Als de PO door drukte slecht bereikbaar is, kan worden overwogen om elke week een vast (digitaal) inloop moment te plannen voor het beantwoorden van vragen uit de organisatie. | 1 2 3 4 |
| Bij het uitvoeren van een DPIA kan het nuttig zijn een multidisciplinair team samen te stellen (bijvoorbeeld: privacy jurist, ICT, initiatiefnemer nieuw proces). Dan kan er snel worden geschakeld en kan de DPIA efficiënt worden uitgevoerd. | 2 3 |
| Stel een proces op waarin de FG in samenwerking met de PO(s) een vaste adviesrol inneemt ter implementatie van PbD in een concreet project. | 1 2 3 4 |

8 Hoewel het proces van afbouw onderdeel vormt van de systeemlevenscyclus, valt dit en processen als Archiving by Design buiten de scope van deze handleiding.

| | | | | |
|---|---|---|---|---|
| Indien gewenst en passend voor de specifieke organisatie, kunnen aanvullende richtlijnen of leg principes worden opgesteld/vastgelegd ter ondersteuning bij de praktische implementatie van PbD in de specifieke organisatie en de bijbehorende dagelijkse praktijk. Houd deze richtlijnen kort en verduidelijk ze met voorbeelden. | 1 | 2 | 3 | 4 |
| Organiseer regelmatig trainingen over privacy en gegevensbescherming waaronder ook PbD. Houd bij wat er in de praktijk met de opgedane kennis wordt gedaan (zie ook de *best practices* rondom onderwijs en bewustwording). | 1 | 2 | 3 | 4 |
| Indien gewenst en passend voor de specifieke organisatie, kan een aanvullend overzicht van PbD *best practices* worden bijgehouden voor een specifieke organisatie en de bijbehorende praktijk. Deze kunnen gegenereerd zijn op basis van ervaring en/ of op basis van inzichten verkregen via ketenpartners en derden en dienen periodiek aangepast of aangevuld te worden afhankelijk van de laatste stand van zaken. Deel deze *best practices* met collega's. | 1 | 2 | 3 | 4 |
| Houd een overzicht van de technische stand van zaken bij, met name een overzicht van de mogelijke technische wijzen voor de implementatie van PbD (PET's). Deze kunnen gegenereerd zijn op basis van ervaring en/ of op basis van inzichten verkregen via ketenpartners en derden en dienen periodiek aangepast of aangevuld te worden afhankelijk van de laatste stand van de techniek. Deel deze met collega's. | 1 | 2 | 3 | 4 |
| PbD geldt voor de hele life cycle van een proces, product, etc. Bepaal van tevoren hoe wordt omgegaan met het dichten van privacy-gerelateerde gebreken in processen en systemen als de looptijd nog niet voorbij is. Dit hangt mede af van het risico van het proces, product, etc. Bepaal wat 'passend' is in die specifieke situatie. | 3 | | 4 | |
| Voer een slagboommodel in waarbij vooraf wordt vastgesteld op welke momenten het noodzakelijk is om naar privacy en security aspecten te kijken. Het proces kan worden gestart met twee zinnen:<br>* naar welk niveau willen we toe: [.....] (op de schaal tussen 100% compliance en 100% niet-compliance)<br>* waar staan we nu [....] (op de schaal tussen 100% compliance en 100% niet-compliance).<br>Maak vervolgens een concrete planning wanneer er geëvalueerd zal worden. | 1 | 2 | 3 | 4 |
| Richt een systeem voor verantwoording in rondom de risico's en zorg er daarbij voor dat verantwoordelijkheden binnen de organisatie breed worden neergelegd. | 1 | 2 | 3 | 4 |
| Maak eventueel gebruik van het crisp-dm model om vorm te geven aan de richtlijnen die rondom PbD in deze handleiding worden gegeven. Zie voor nadere uitleg rondom het crisp-dm model Bijlage B. | 1 | 2 | 3 | 4 |
| <<< Ruimte voor nieuwe *best practices* >>> | 1 | 2 | 3 | 4 |

**VOORBEELD**
Organisatie x koopt regelmatig via aanbestedingsprocedures nieuwe applicaties. De FG van Organisatie x wordt al bij het aanbestedingstraject betrokken zodat deze kan meekijken en adviseren over privacy-aspecten, waaronder PbD.

### Inrichting draagvlak bestuur/directie

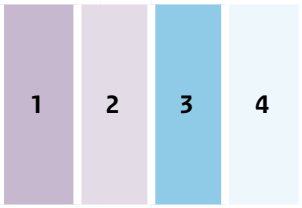
| | | | | |
|---|---|---|---|---|
| Maak als bestuur/directie het gebruik van veilige en gemeenschappelijke methodes een doel. Daarbij dient ook het gesprek te worden gevoerd t.a.v. welke privacy risico's wel en niet kunnen worden genomen. Het identificeren van de grootste risico's is daarbij belangrijk. | **1** | 2 | 3 | 4 |
| Vergroot het draagvlak binnen de organisatie voor de implementatie van PbD, bijvoorbeeld via casusbesprekingen per afdeling om vast te stellen wat goed gaat en waar de verbeterpunten liggen. | **1** | 2 | 3 | 4 |
| Stel als bestuur/directie "business requirements" op waarin baseline wettelijke verplichtingen, waaronder ook PbD (artikel 25 AVG), voorop worden gesteld. Als de wens er is om dit niet als requirements (verplichtingen) vast te leggen, maar als richtlijnen of uitgangspunten, kan dat ook. | **1** | 2 | 3 | 4 |
| Stel als bestuur/direct het aanmoedigen en stimuleren van de intrinsieke motivatie bij medewerkers rondom de implementatie van PbD centraal door commitment in te bouwen in alle lagen van de organisatie. Concrete voorbeelden die bij medewerkers tot de verbeelding spreken heeft daarbij de voorkeur. | **1** | 2 | 3 | 4 |
| Wees als directie/bestuur actief betrokken op verschillende lagen binnen de organisatie bij discussie rondom PbD en de praktische – en vooral ook passende - implementatie daarvan. | **1** | 2 | 3 | 4 |
| Stel duidelijk beleid op dat specifiek toeziet op PbD of waarin PbD al doelstelling en aandachtspunt wordt benoemd. Maak gebruik van de kracht van herhaling. | **1** | | | |
| <<< Ruimte voor nieuwe *best practices* >>> | **1** | 2 | 3 | 4 |

**VOORBEELD**
Medewerkers in organisatie X ervaren veel druk van het bestuur dat PbD "nu echt moet worden toegepast". Medewerkers hebben de indruk dat PbD voor bestuurders een buzzword is, en zij niet weten wat het voor de praktijk betekent. Op initiatief van de medewerkers wordt een bespreking met het bestuur ingepland en worden een aantal concrete casussen besproken waar medewerkers tegenaan lopen. Het bestuur begrijpt de praktijk nu beter en kan gerichter sturen.

### Inrichting interne documentatie

| | | | | |
|---|---|---|---|---|
| Zorg ervoor dat de interne documentatie goed op orde is en dat iedereen deze kan vinden. Gebruik een versiemanagementsysteem. | **1** | 2 | 3 | 4 |
| Stel een datalekprotocol op en zorg dat iedereen deze kan vinden. Houd dit datalekprotocol actueel. | 2 | **3** | 4 | |
| Stel een lijst van goedgekeurde instrumenten en bibliotheken op, bijvoorbeeld: code bibliotheek, programmeertaal, versie beheerssysteem, testinstrumenten, infrastructuur, controle-instrumenten, logboekserver, kader van derden en API's. **Let op**: als hiervoor wordt gekozen, moet dit niet aan innovatie in de weg staan. Deze lijst kan alleen dienen ter indicatie of een eerste denkstap bieden. Als er een lijst wordt gebruikt, is het van belang deze levendig en up to date te houden. Er kan ook worden gekozen om aan te sturen op principes. | **1** | | | |

Let op met het gebruiken van steeds dezelfde lijsten: generieke lijsten met eisen voor partijen die zich inschrijven op aanbestedingen zijn handig, maar bij PbD is het wel van belang om dat kritisch te bekijken. De lijsten kunnen een eigen leven gaan leiden als ze gewoon klakkeloos worden toegepast. Ook kan PbD in de ene aanbesteding anders worden uitgelegd dan in de andere. Het gaat er weer om wat 'passend' is voor die specifieke situatie.




Gebruik goedgekeurde tools en frameworks.


<<< Ruimte voor nieuwe *best practices* >>>

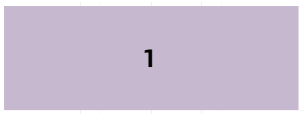

**VOORBEELD**
Organisatie X koopt regelmatig applicaties van derden. Omdat er wordt opgemerkt dat bij iedere aanbesteding het wiel opnieuw moet worden uitgevonden, wordt er een checklist opgesteld met minimale vereisten op het gebied van privacy en security waar de nieuwe leverancier aan moet voldoen. Deze checklist is zowel voor de inkoper, de privacy expert en de security expert goed vindbaar.

Organisatie X staat op het punt een nieuwe kern applicatie aan te kopen, waar heel veel bijzondere persoonsgegevens van burgers in zullen worden verwerkt. Op dat idee is een DPIA uitgevoerd. De risico's die uit deze DPIA komen, worden gelegd tegen het lijstje voor de aanbesteding. Op een paar punten wordt het lijstje aangepast en de aanbesteding wordt uitgezet.

In het standaardlijstje wordt aangepast dat wanneer er veel bijzondere persoonsgegevens in de applicatie worden verwerkt, er aanvullend aandacht moet worden besteed aan punten 1, 2 en 3.

### Inrichting assessments, logging en audits

Voer een quick-scan DPIA uit wanneer dit nodig wordt geacht. Bij twijfel is het beter om een quick-scan uit te voeren dan het te laten zitten. Later bijsturen op het gebied van privacy is namelijk moeilijker dan bijsturen aan het begin.




Voer een DPIA uit wanneer dit vereist is. Werk waar mogelijk met een multidisciplinair team.


Zorg ervoor dat DPIA's niet te smal of te breed gescoped worden. Zo kan er bijvoorbeeld voor worden gekozen om een DPIA op één hoog risico verwerking uit te voeren, in plaats van het gehele systeem.


Voer (interne) privacy audits uit.

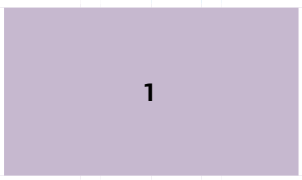

Voer security checks en dreigingsanalyses uit voor de software.


Log welke medewerkers toegang verkrijgen tot welke bronnen.


Houd statistieken bij: hoeveel DPIA's worden uitgevoerd, hoeveel quick-scan DPIA's worden uitgevoerd?


Verhelder en stel vast wat de risicobereidheid, oftewel welke risico's geaccepteerd worden en onder welke omstandigheden.


Verhelder en stel vast wat de procedure is rondom en afweging tussen wat mogelijk is en wat nodig is bij de ontwikkeling van nieuwe systemen en processen waarbinnen persoonsgegevens worden verwerkt. Zorg dat de mogelijkheid wordt geopend om hier een gesprek over te hebben, in plaats van de AVG zo streng mogelijk proberen uit te leggen.



<<< Ruimte voor nieuwe *best practices* >>>

| 1 | 2 | 3 | 4 |
|---|---|---|---|

**VOORBEELD**
Organisatie X beseft dat het uitvoeren van DPIA's heel veel tijd kost, en wil voorkomen dat er onnodige DPIA's worden uitgevoerd. Daarom stelt organisatie X een quick-scan op met vragen toegespitst op de organisatie of een DPIA wel of niet moet worden uitgevoerd. De FG in de organisatie houdt eens per kwartaal een steekproef bij een aantal quick-scan resultaten of het inderdaad klopt dat er wel of geen DPIA is uitgevoerd.

De statistieken worden bijgehouden in een logboek (hoeveel quick-scans, hoeveel DPIA's).

## Inrichting informatieplicht

| | | | | |
|---|---|---|---|---|
| Stel een duidelijke privacyverklaring op die makkelijk toegankelijk is. | | 2 | 3 | 4 |
| Implementeer een richtlijn dat ieder document dat wordt gebruikt voor betrokkenen, in een eenvoudige tekst wordt opgesteld. | | 2 | 3 | 4 |
| <<< Ruimte voor nieuwe *best practices* >>> | 1 | 2 | 3 | 4 |

## Samenwerking met externe partijen

| | | | | |
|---|---|---|---|---|
| Zorg ervoor dat de kwalificering van de rollen van alle betrokken partijen (gebruiker, beheerder, betrokkene) al vroegtijdig in iedere fase helder is voor partijen. | 1 | 2 | 3 | 4 |
| Zorg ervoor dat alle relevante externe stakeholders vroegtijdig bij de inrichting van het proces betrokken worden. | 1 | | 2 | |
| Stel eisen uit vooraf goedgekeurde tools en frameworks aan externe partijen, bijvoorbeeld leveranciers ("checklist"). | | 2 | 3 | |
| Sluit met iedere verwerker een verwerkersovereenkomst, bijvoorbeeld op basis van het model van de Rijksoverheid. Wees daarbij ook kritisch. Er zijn externe partijen die aannemen dat ze verwerker zijn, terwijl ze in de werkelijkheid verwerkingsverantwoordelijke zijn. Bij twijfel overleg met de PO. | | 2 | 3 | |
| Stel contractueel vast wie als Trusted Third Parties beschouwd kunnen worden. | | 2 | 3 | |
| Zorg ervoor dat bij nieuwe aanbestedingen leveranciers worden uitgevraagd over de wijze waarop deze kan voldoen aan de vereisten rondom PbD aan de hand van vooraf opgestelde "requirements". Enkel een vakje aanvinken dat 'men voldoet aan PbD' is dus niet genoeg; maak het concreet. Dit kan aan de hand van een user case, bijvoorbeeld: kan de leverancier aantonen dat de app een privacy dashboard zal bevatten waarmee de betrokkene met één druk op de knop zijn persoonsgegevens kan laten aanpassen. | | 2 | 3 | |
| Verplicht de een externe leverancier om documentatie aan te leveren waarin de genomen privacy maatregelen worden beschreven. Dit kan ook als onderdeel van de verwerkersovereenkomst of andere (data)overeenkomst worden opgeleverd. Bevraag die documentatie kritisch waar nodig. | | 2 | 3 | |

Leg in contractbepalingen vast dat partijen verplicht zijn de data te anonimiseren of pseudonimiseren en anoniem of pseudoniem te houden. Vraag goed door of de externe partij anonimiseert wanneer dat is overeengekomen en dat het niet (toch) om pseudonimiseren gaat.


Betrekt waar nodig de Autoriteit Persoonsgegevens (AP).


Werk samen met ketenpartners om het draagvlak en bewustzijn onder medewerkers te vergroten en het delen van kennis en ervaring rondom de praktische implementatie van PbD te faciliteren.


Houd een gesprek met de leverancier waar een systeem halverwege de levensloop niet meer goed werkt en zorg ervoor dat processen in de tussentijd waar nodig worden aangepast.

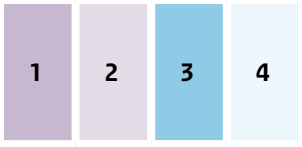

Ontwikkel een praktische werkwijze (op ketenniveau) om *best practices* rondom nieuwe ontwikkelingen tussen ketenpartners te delen.


<<< Ruimte voor nieuwe *best practices* >>>


**VOORBEELD**
Organisatie X besteedt een aantal belangrijke verwerkingen uit aan Verwerker Q. Tijdens het afsluiten van de verwerkersovereenkomst meldt verwerker Q. dat zij alle passende maatregelen zal nemen om de persoonsgegevens te beveiligen. Organisatie X vraagt vervolgens door wat de belangrijkste maatregelen zijn en waarom zij passend zijn.

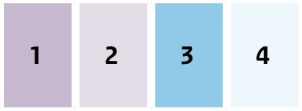
### Inrichting onderwijs en facilitering van bewustwording

Zorg ervoor dat het bij iedere stakeholder duidelijk is wat in een bepaald geval onder PbD moet worden verstaan. Probeer het zo concreet mogelijk te maken hoe het in een specifiek proces uitziet. De voorkeur verdient een praktische omschrijving boven een perfect geformuleerd theoretisch antwoord.

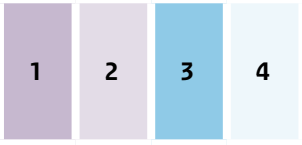



Richt een trainingsprogramma rondom privacy en gegevensbescherming in, waarin ook wordt stilgestaan bij PbD.


Zorg ervoor dat mensen binnen de organisatie geïnformeerd zijn en blijven over PbD, bijvoorbeeld via het cursussen, workshops, intervisiesessies, regelmatige herhaling, persberichten en informatie via het intranet.

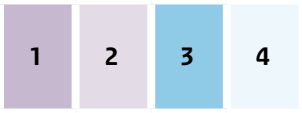



Zorg ervoor dat er binnen trainingsprogramma's ruimte is om medewerkers te informeren maar ook om medewerkers onderling proactief te laten brainstormen over mogelijke manieren waarop processen en systemen in overeenstemming met PbD kunnen worden ingericht.




Faciliteer samenwerking met externe partijen om meer over PbD te leren (bijv. externe trainingen).


Ondersteun medewerkers middels tekstuele en visuele bronnen en materialen rondom privacy en PbD (bijv. handouts), waarin concrete handvatten worden geboden om PbD in concrete gevallen te implementeren.



| | | | | |
|---|---|---|---|---|
| Bouw een proces van verantwoording op aan de hand waarvan kan worden vastgesteld dat een training is gegeven en ook kan worden verzekerd dat naar aanleiding van de training een vertaalslag naar de praktijk wordt gemaakt. Dit kan bijvoorbeeld door het uitreiken van een checklist op het gebied van PbD die de medewerkers de volgende keer dat ze een proces starten, moeten invullen. | 1 | 2 | 3 | 4 |
| Verhelder de scope van PbD en hoe deze verplichting zich verhoudt tot de AVG en andere relevante wettelijke kaders (bijvoorbeeld de Wpg en de Wjsg). | 1 | 2 | 3 | 4 |
| Maak het voor teams die PbD implementeren in de praktijk om hierbij praktische ondersteuning te krijgen, bijvoorbeeld via scrums en agile teams. Dat betekent dat een groot project in kleine stukjes wordt opgedeeld en elke x aantal weken – bijvoorbeeld 3 – aan het kleine stukje wordt gewerkt en er vervolgens een nieuw klein stukje in een 3-weekse cyclus wordt opgepakt. | 1 | 2 | 3 | 4 |
| Zorg ervoor dat de POs – die als eerste aanspreekpunt fungeren voor privacy-gerelateerde vraagstukken binnen de organisatie - voldoende op de hoogte zijn van de passende maatregelen die de implementatie van PbD ondersteunen. | 1 | 2 | 3 | 4 |
| <<< Ruimte voor nieuwe *best practices* >>> | 1 | 2 | 3 | 4 |

### Inrichting software-instellingen

**LET OP**: deze handleiding omvat geen concrete technische keuzes. Wat er in deze paragraaf aan bod komt, betreffen uitgezoomde aandachtspunten:

- Zorg ervoor dat het in het geval van pseudonimisering niet mogelijk is om de originele data terug te halen zonder autorisatie.
- Zorg ervoor dat de software beveiligd is bij het opslaan van data, bijvoorbeeld middels encryptie.
- Zorg ervoor dat de software de integriteit van de data waarborgt.
- Zorg ervoor dat de software kan detecteren wanneer er wijzigingen worden aangebracht in bestande, services en netwerken door:
  - het vergelijken van hashwaarden en checksums;
  - het beperken van schrijftoegang;
  - regelmatige integriteitscontroles;
  - het instellen van referentiewaarden (min/max).
- Zorg ervoor dat de software toegang geeft tot persoonsgegevens wanneer dat nodig wordt geacht.
- Zorg ervoor dat het softwarebestand is tegen bedreigingen. Denk hierbij aan:
  - beveiliging tegen bekende veiligheidslekken en kwetsbaarheden;
  - correcte configuratie;
  - segmentatie van opgeslagen gegevens, systemen, verwerkers en netwerken;
  - het up-to-date houden van software van derden en patches;
  - stel de relevante personen in staat om meldingen van gebruikers en anderen over kwetsbaarheden in de software te ontvangen en ervoor te zogen dat deze worden beheerd en serieus worden genomen.
  - de veilige vernietiging van media waarmee persoonsgegevens worden verwerkt.
- Schakel onnodige tracking, logging en verzameling van persoonsgegevens uit.
- Doe een handmatige codecontrole.
- Controleer de gehele gegevensstroom.
- Integreer de privacy vereisten in de code.

**LET OP**: Zorg ervoor dat privacy niet ten koste gaat van functionaliteit. Medewerkers moeten ook hun werk kunnen blijven uitoefenen. Privacybescherming dient passend te zijn, niet op alle vlakken het hoogste niveau van bescherming dat technisch mogelijk is, aangezien de AVG dit niet vereist, maar deze maatregelen ook veel middelen en tijd kosten. Ga hierover het gesprek aan.

Zie voor achtergrondinformatie over de verantwoordingsplicht onder de AVG paragraaf 5.2 van deze handleiding.

## 3.3. Stap 3: Documenteer de genomen maatregelen

Documentatie van de genomen maatregelen is noodzakelijk omdat:

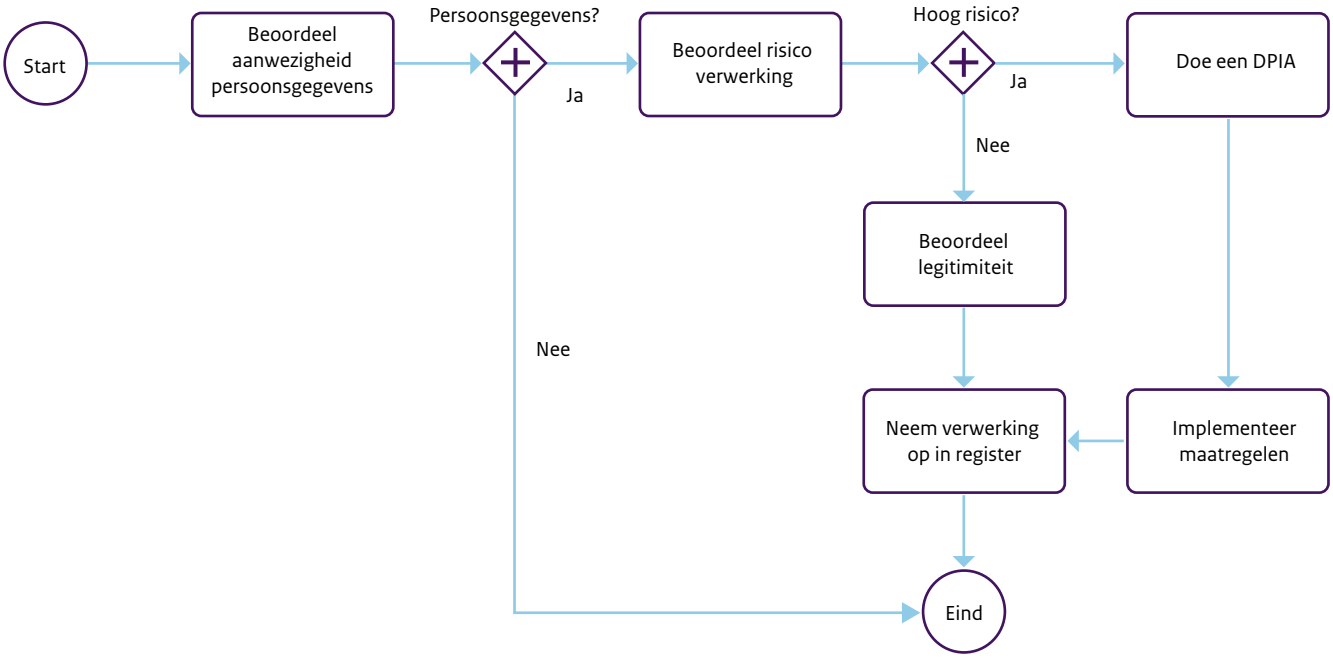
- achteraf moet kunnen worden uitgelegd waarom een bepaalde maatregel is genomen;
- controle moet kunnen plaatsvinden dat de maatregel daadwerkelijk is genomen;
- leren van genomen maatregelen voor toekomstige situaties (wat werkt wel, wat werkt niet).

Deze drie punten zijn ook in de AVG vastgelegd in artikel 5 lid 2 AVG als de 'verantwoordingsplicht'. De verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de gegevensbeschermings-beginselen en die naleving moet aantonen (verantwoordingsplicht).

Zie voor achtergrondinformatie over de verantwoordingsplicht onder de AVG paragraaf 6.1.7 van deze handleiding.

Het documenteren van de genoemde maatregelen kan via een DPIA. In de DPIA worden genomen maatregelen gedocumenteerd en de geïmplementeerde maatregelen dienen vervolgens ter documentatie in het verwerkingsregister te worden opgenomen. Dit proces van documentatie en verantwoording kan als volgt worden weergegeven:

**Figuur 3.5.** Project definiëring, risicobeoordeling en implementatie mitigerende maatregelen.



# DEEL II | theoretische verdieping rondom PbD

# 4. PbD en de bescherming van persoonsgegevens

## 4.1. Wat is PbD?

**PbD is**: gegevensbescherming door ontwerp.

**Artikel in de AVG**: artikel 25 lid 1 AVG.

**In de kern betekent dit**: organisaties die met persoonsgegevens werken moeten in een zo vroeg mogelijk stadium (proactief) in het ontwerp van systemen, applicaties, processen, beleid en (ICT) producten waarbij persoonsgegevens worden verwerkt, passende waarborgen inbouwen (in het ontwerp) om privacy te beschermen.

Voorbeelden van '**zo vroeg mogelijk**'

Wanneer...

| | |
|---|---|
| ...methodes voor de verwerking worden gewijzigd | ...gebruikt wordt gemaakt van externe leveranciers die toegang hebben tot persoonsgegevens of deze gebruiken en/of opslaan |
| ...initiatief is genomen voor een nieuw proces waarbij persoonsgegevens worden verwerkt | ...systemen met persoonsgegevens buiten gebruik worden gesteld |
| ..... er sprake is van een nieuw bedrijfsproces dat een significante nieuwe verzameling, gebruik of openbaarmaking van persoonsgegevens met zich meebrengt | ... meerdere databanken met persoonsgegevens worden samengevoegd of er een plan is om persoonsgegevens uit openbare of commerciële bronnen/databanken op te nemen in een bestaande databank |

| **Voorbeeld: op tijd betrokken** | **Voorbeeld: te laat betrokken** |
|---|---|
| Er is een idee voor een nieuwe applicatie. De initiatiefnemer bespreekt dit idee met de PO en vraagt welke privacy implicaties de PO ziet. De PO ziet een aantal knelpunten. De initiatiefnemer past daarop het plan aan. | In het beleid zijn alle keuzes al gemaakt, onder meer welke persoonsgegevens zullen worden verwerkt, wat de applicatie moet gaan doen en wat de einddoelen zijn. Er moet nog wel 'even' een DPIA gedaan worden. Uit de DPIA komen verschillende risico's naar voren, maar de applicatie is al ontworpen en kan niet zonder veel tijd en middelen weer worden aangepast. |
| Er kan op dit punt op tijd worden bijgestuurd. | Er kan op dit punt moeilijk worden bijgestuurd. |

## 4.2. Hoe verhoudt PbD zich tot de privacybeginselen?

De AVG schrijft voor dat de verwerking van persoonsgegevens rechtmatig en behoorlijk moet zijn.

'**Rechtmatig**' betekent: de gegevensverwerking moet gebaseerd zijn op een rechtsgrond uit artikel 6 AVG; de juridische reden waarom persoonsgegevens worden verwerkt.

Zie voor achtergrondinformatie over het rechtmatigheidsprincipe paragraaf 6.1.1 van deze handleiding.

'**Behoorlijk**' betekent: de gegevensverwerking moet, naast rechtmatigheid, ook aan andere vereisten voldoen; de juridische zorgvuldigheidseisen van een gegevensverwerking. Er moet dus worden aangetoond dat de gegevensverwerking niet alleen rechtmatig is, maar ook dat de gegevensverwerking op een behoorlijke manier plaatsvindt.

De behoorlijkheidsvereisten worden ook 'privacybeginselen' genoemd en zijn neergelegd in artikel 5 AVG. De privacybeginselen zijn nader uitgewerkt in andere bepalingen uit de AVG.

De privacybeginselen uit **artikel 5 AVG**:

- **Rechtmatig, behoorlijkheid en transparantie**: de persoonsgegevens moeten op een rechtmatige en eerlijke wijze worden verwerkt.
- **Doelbinding**: de persoonsgegevens moeten worden verwerkt voor bepaalde doeleinden en mogen niet verder worden verwerkt als het niet overeenstemt met deze doeleinden.
- **Minimale gegevensverwerking**: er mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het beoogde doel van de verwerking te bereiken.
- **Juistheid**: persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd.
- **Opslagbeperking**: persoonsgegevens moeten verwijderd worden wanneer zij niet langer nodig zijn om het beoogde doel te bereiken.
- **Integriteit en vertrouwelijkheid**: de beveiliging van persoonsgegevens gewaarborgd worden door middel van passende technische en organisatorische waarborgen.
- **Verantwoordingsplicht**: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en kan dit aantonen.

Er bestaat geen rangorde in deze beginselen.

Rechtmatigheid en behoorlijkheid zijn allebei nodig om te kunnen spreken van een 'goede' gegevens-verwerking. Hieronder worden twee voorbeelden gegeven, toegespitst op PbD, waarbij ofwel de rechtmatigheid ofwel de behoorlijkheid ontbreekt.

| Voldaan aan rechtmatig | + | niet voldaan aan behoorlijk | = | geen ‘goede’ gegevensverwerking |
|---|---|---|---|---|

**VOORBEELD**
X verwerkt op grond van haar wettelijke taak medische persoonsgegevens van justitiabelen met het oog op de vertrekking van medische zorg tijdens het verblijf in een justitiële inrichting (toelichting: rechtsgrond is aanwezig). Het systeem waarin de gegevens zijn opgeslagen, wist na afloop van de bewaartermijn de gegevens niet automatisch, terwijl X ervanuit ging dat dit wel het geval was omdat de leverancier van het systeem had aangegeven dat het systeem aan PbD voldeed (toelichting: persoonsgegevens worden door een ontwerp- en communicatie issue niet automatisch gewist, hetgeen in dit geval niet voldoet aan beginselen uit artikel 5 AVG).

| Niet voldaan aan rechtmatig | + | Voldaan aan behoorlijk | = | geen ‘goede’ gegevensverwerking |
|---|---|---|---|---|

**VOORBEELD**
verwerkt de medische gegevens van justitiabelen en deelt deze met commerciële partijen voor commerciële doeleinden, namelijk kortingen op producten en diensten (toelichting: hiervoor is geen rechtsgrond aanwezig). Voor de verkoop exporteert X een bestand uit haar systeem. Het systeem laat het echter niet toe om alle gegevens te exporteren. Vervelend voor X, want als dat wél mogelijk was geweest, zou zij meer inkomsten kunnen genereren (toelichting: doordat het systeem zo ontworpen is dat het niet mogelijk is om alle persoonsgegevens te exporteren en in dit geval voor onrechtmatige doeleinden te verwerken, is dit ontwerp in dit geval te beschouwen als een ontwerp waarin de beginselen uit artikel 5 AVG zijn meegenomen).

Hoe beter PbD wordt toegepast, hoe beter de beginselen uit de AVG (artikel 5 AVG) kunnen worden nageleefd. Begrip van de beginselen uit artikel 5 AVG is belangrijk om PbD toe te kunnen passen. Toelichting: bij een goede toepassing van PbD zal voordat het ontwerpproces aanvangt en gedurende het ontwerpproces steeds de vraag worden gesteld of het echt noodzakelijk is om (bepaalde) persoonsgegevens te verwerken (dit matcht met ‘minimale gegevensverwerking’), hoe de gegevens het best beveiligd kunnen worden (dit matcht met ‘integriteit en vertrouwelijkheid’) en hoe persoonsgegevens na verloop van tijd het best opgeslagen of verwijderd kunnen worden (dit matcht met ‘opslagbeperking’).

De privacybeginselen schrijven voor dat de beginselen door de verwerkingsverantwoordelijke moeten worden nageleefd en dat dit moet worden aangetoond. PbD draagt bij aan een effectieve uitvoering van de privacybeginselen.

De rol van PbD binnen de systeemlevenscyclus wordt verder besproken in paragraaf 5.3 van deze handleiding.

De rol van de privacybeginselen in het kader van PbD wordt verder besproken in hoofdstuk 5 van deze handleiding.

## 4.3. PbD, ontwerpstrategieën en PET's

**Figuur 4.1.** AVG-normen, ontwerpstrategieën en PET's.


De AVG schrijft niet voor hoe je PbD in de praktijk moet of kunt toepassen. Er zijn PbD ontwerpstrategieën ontwikkeld die een nadere invulling geven door middel van concrete ontwerpeisen die een privacy-vriendelijke invulling geven aan de technische en organisatorische samenstelling van een systeem. Het uitgangspunt hierbij is dat een organisatie passende technische en organisatorische maatregelen neemt om ervoor te zorgen dat eventuele inbreuken op de privacy van individuen zo veel mogelijk wordt beperkt. Aan deze ontwerpstrategieën kan in de praktijk invulling gegevens middels privacybeschermende technologieën (ook wel 'PET('s)' genoemd).[9] PET's zijn verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen.

9 PET's richten zich op het elimineren en minimaliseren van persoonsgegevens. PET's zullen geen oplossing zijn voor alle privacyrisico's.

# 5. PbD: nadere uitleg en concrete stappen

## 5.1. Vuistregels voor PbD

De volgende vuistregels kleuren PbD in (zie figuur 5.1).

**Figuur 5.1.** De PbD-vuistregels.

| | |
|---|---|
| 1 | Proactief niet reactief |
| 2 | Privacy als standaardinstelling |
| 3 | Privacy ingebouwd in design |
| 4 | Positieve benadering privacy |
| 5 | Bescherming hele cyclus |
| 6 | Zichtbaarheid en transparantie |
| 7 | Respect voor privacy betrokkenen |

## 5.2. Hoe aan de vuistregels te voldoen?

Door het identificeren, implementeren en toepassen van **passende technische** (o.a. systeemeisen, beveiligingseisen, autorisaties) en **organisatorische maatregelen** (o.a. werkprocessen, *checks and balances*, trainingen).[10]

In de AVG is het woord "passend" niet gedefinieerd en er zijn ook geen voorbeelden gegeven van technische- en of organisatorische maatregelen.

Wel zijn er aspecten geformuleerd om te bepalen wat "passend" is in een bepaald geval:

- de **stand van de techniek** (*state of the art* – zie hierna);
- de **uitvoeringskosten** (bronnen en mensen);
- de **aard** (de kernmerken) van de verwerking;
- de **omvang** (omvang en bereik) van de verwerking;
- de **context** (omstandigheden rondom de verwerking die de verwachtingen van betrokkenen kunnen beïnvloeden) van de verwerking;
- het **doel** (op welke doelstellingen heeft de verwerking betrekking) van de verwerking; en
- de **risico's voor de betrokkene**.

Wat een "passende" maatregelen in 2020 was, hoeft dat niet meer in 2025 te zijn. Belangrijk is dus om de maatregelen periodiek onder de loep te nemen.

10 EDPB; richtsnoeren 4/2019 inzake artikel 25, vastgesteld op 20 oktober 2020, randnummer 7, p. 6.

Bij het bepalen van wat wel en niet "passend" is en hoe aan de PbD vuistregels voldaan kan worden, kunnen de in tabel 5.1 opgenomen stappen helpen. Deze stappen dienen zo vroeg mogelijk (proactief) in het proces waarbij persoonsgegevens een rol spelen, te worden doorlopen. Dit is niet vermeld bij elke stap.

**Tabel 5.1.** Aanvullende factoren bepaling 'passende technische en organisatorische maatregelen'.

| | | |
|---|---|---|
| 1 | Bepaal of het nodig is om een gegevensbeschermingseffectbeoordeling (hierna: "DPIA")[11] uit te voeren. Gebruik daarvoor een checklist die als uitkomst geeft of het wel of niet nodig is een DPIA uit te voeren.[12]<br><br>Zie dit niet als een 'moetje' of onderdeel van een 'afvinklijstje', maar als een kans om een serieus gesprek te voeren over de risico's.<br><br>**Actie**:<br>Indien er geen checklist bestaat: stel er een op en maak het onderdeel van het proces. Noem daarbij ook een contactpersoon die mee kan denken of het uitvoeren van een DPIA wel of niet nodig is. | Vuistregels 1, 2 en 3. |
| 2 | Bepaal (kritisch) of een bepaalde gegevensverwerking überhaupt noodzakelijk of wenselijk is. Is het 'need to have' of 'nice to have'. Als het een 'nice to have' is en er is geen andere goede (objectieve) reden om de persoonsgegevens te verwerken, verwerk die persoonsgegevens dan niet. Identificeer waar de knelpunten zitten, pas aan en stel opnieuw de vraag, net zolang tot alle persoonsgegevens die worden verwerkt 'need to have' zijn.<br><br>In de meeste processen van JenV worden persoonsgegevens op basis van een wettelijke taak verwerkt. Dat betekent dat de wet voorschrijft welke persoons-gegevens nodig zijn 'need to have'. De rest is hoogstwaarschijnlijk 'nice to have'.<br><br>**Een alternatief**:<br>In plaats van persoonsgegevens kunnen ook geanonimiseerde gegevens worden gebruikt (AVG niet van toepassing).<br><br>In plaats van 10 verschillende soorten persoonsgegevens te verwerken, kan er misschien ook worden volstaan met 8 verschillende soorten persoonsgegevens. | Vuistregels 1, 2, 3, 4 en 7. |
| 3 | Voer een nulgesprek waarbij POs met medewerkers en management van de eerste lijn samen nagaan wat de privacy implicaties van een bepaalde verwerking zouden kunnen zijn. | Vuistregels 1, 4 en 7. |
| 4 | Betrek de Functionaris Gegevensbescherming (hierna: "FG"). | Vuistregels 1, 4 en 7. |
| 5 | Zorg voor voldoende capaciteit (mensen, middelen) dat PbD ook daadwerkelijk in de praktijk kan worden gebracht. | Vuistregels 1 en 5. |
| 6 | Verzeker dat privacy en gegevensbescherming bij bestuur en directie geprioriteerd worden, ook gelet op punt 5. | Vuistregels 1 en 4. |

11 **Let op**: op basis van de AVG is een DPIA in een aantal gevallen verplicht (zie artikel 35 AVG), bijvoorbeeld wanneer de verwerking een 'hoog risico' inhoudt. In aanvulling op de wettelijke bepaling van artikel 35 AVG zijn er verschillende checklists (Pre-DPIA's) die hierop sturen. Zie hierover ver paragraaf 6.1.

12 Zie bijvoorbeeld de DPIA-checklist van de Autoriteit persoonsgegevens https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/schema_dpia_na_25_mei.pdf. Zie ook het format pre-DPIA scan van CIPP-Overheid https://www.cip-overheid.nl/media/1774/20220301-format-pre-scan-dpia-cip-v34-def.xltx.

| | | |
|---|---|---|
| **7** | Besef dat veel systemen die worden gebruikt, zijn ontworpen voor de intreding van de AVG. Sommige van deze systemen zijn zo ontworpen dat bepaalde PbD beginselen daarin nog niet zijn meegenomen. Identificeer knelpunten en weeg af hoe erg die knelpunten zijn. Kan de verbetering worden meegenomen bij een nieuw systeem of moeten in het oude systeem toch wijzigingen worden doorgevierd? | Vuistregels 5, 6 en 7. |
| **8** | Kies als organisatie één lijn. Wat is acceptabel en wat niet? De mening van individuele medewerkers kan worden meegenomen om de lijn te bepalen en te evalueren. | Vuistregel 1. |
| **9** | Prioriteer privacyvraagstukken, ook als dat betekent dat er minder tijd aan andere processen kan worden besteed. | Vuistregels 1, 5 en 7. |

"Passend" en PbD brengen **niet** mee dat de bescherming van privacy altijd op de meest strenge manier moet worden toegepast of dat de AVG op de meest strenge manier moet worden uitgelegd. Het betekent dat de privacy, op de best mogelijke manier die past bij de specifieke situatie, moet worden geborgd bij het ontwerp van processen, producten, etc.

PbD betekent dus niet dat het alleen 'goed' is als de meest strenge uitwerking van maatregelen wordt gekozen. Soms is dat nodig, omdat het in dat geval passend is. In andere gevallen zijn lichtere maatregelen juist passend.

Hieronder een voorbeeld om dit verschil te illustreren:

In een systeem van organisatie X worden de naam het adres en de geboortedatum van burgers verwerkt om verzoeken van burgers op gebied Y te kunnen beoordelen.

Organisatie X voldoet aan de beginselen van rechtmatigheid en behoorlijkheid, maar heeft vernomen dat PbD ook heel belangrijk is en vraagt zich af of daaraan is voldaan.

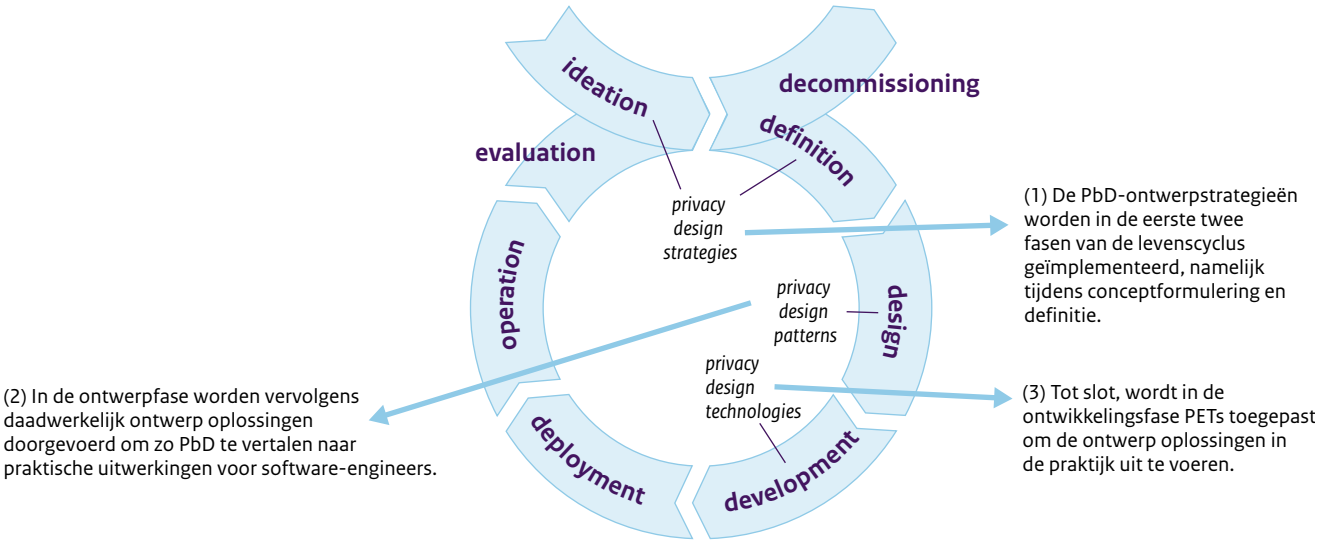
| "passend" is niet meegenomen | "passend" is wel meegenomen |
|---|---|
| Voor de zekerheid blokkeert de beheerder de toegang voor alle medewerkers die zich bezig houden met de behandelingen van de verzoeken van burgers op gebied Y. Ook past de beheerder een ingewikkelde en dure vorm van encryptie toe om er zeker van te zijn dat de verzoeken van burgers op gebied Y niet zo gemakkelijk kunnen worden geopend.<br><br>De medewerkers ervaren door deze maatregelen hindernissen bij hun dagelijkse werkzaamheden.<br><br>Er worden bovendien hoge kosten gemaakt, terwijl dit niet nodig is. | Daarom gaat de beheerder na of alle medewerkers die nu toegang hebben tot de verzoeken van burgers op gebied Y, deze toegang ook echt nodig hebben. Daaruit blijkt dat een van de medewerkers, een secretariële kracht, geen toegang nodig heeft tot de verzoeken van burgers. De beheerder blokkeert de toegang voor deze specifieke medewerker.<br><br>Verder komt organisatie X er in gesprekken met de PO en de uitvoering achter dat de naam en de geboortedatum van de burger apart kunnen worden opgeslagen van het adres van de burger, zodat die gegevens minder makkelijk te koppelen zijn. Er worden daarom twee databases aangemaakt.<br><br>De medewerkers ervaren door deze maatregelen geen hindernissen bij hun dagelijkse werkzaamheden.<br><br>Er worden geen onnodige hoge kosten gemaakt. |

## 5.2. PbD gedurende de systeemlevenscyclus

PbD moet worden toegepast in alle fasen van de **systeemlevenscyclus** (waaronder inkoop, aanbestedingen, uitbesteding, ontwikkeling, ondersteuning, onderhoud, testen, opslag, vernietiging enz.). Iedere fase vraagt om aandacht voor de bescherming van de privacy van betrokkenen (zie figuur 5.2).

De PbD-ontwerpstrategieën worden in de eerste twee fasen van de levenscyclus geïmplementeerd, namelijk tijdens conceptformulering en definitie (1). In de ontwerpfase worden vervolgens daadwerkelijk ontwerpoplossingen doorgevoerd om zo PbD te vertalen naar praktische uitwerkingen voor software-engineers (2). Tot slot, wordt in de ontwikkelingsfase PET's toegepast om de ontwerpoplossingen in de praktijk uit te voeren (3).

**Figuur 5.2.** De implementatie van PbD gedurende de systeemlevenscyclus. [13]




Door de ontwerpstrategieën toe te passen wordt concreter invulling gegeven aan het PbD in de ontwerpfase. In hoofdstukken 2 en 6 van deze handleiding wordt verder uitleg gegeven aan deze ontwerpsWtrategieën en de beginselen uit artikel 5 AVG.

13 Deze afbeelding is afkomstig uit Het Blauwe Boekje geschreven door dhr. dr. J.H. Hoepman, 27 januari 2020.

# 6. Privacybeginselen in relatie tot PbD: nadere uitleg en concrete stappen

De beginselen zijn besproken in paragraaf 4.2 en zijn neergelegd in artikel 5 AVG.

Hierna wordt op ieder beginsel ingegaan en wordt uitgelegd hoe dat beginsel zich verhoudt tot PbD. Voor ieder beginsel wordt een aparte paragraaf gebruikt.

## 6.1. Privacybeginselen

### 6.1.1. Rechtmatig, behoorlijk en transparant (artikel 5 lid 1 onder a AVG)

**Kern**: is mijn (beleids)doel rechtmatig, behoorlijk en transparant?

**Let op**: dit beginsel kan wat verwarrend zijn omdat het de woorden 'rechtmatig' en 'behoorlijk' omvat. Artikel 6 AVG verwijst ook naar de 'rechtmatigheid' van de gegevensverwerking, en alle beginselen uit artikel 5 AVG samen worden ook wel de 'behoorlijkheid' van een gegevensverwerking genoemd.

Het **rechtmatigheidsprincipe** beantwoordt de vraag of er een wettelijke rechtsgrond is waarop de verwerking van persoonsgegevens gebaseerd kan worden.

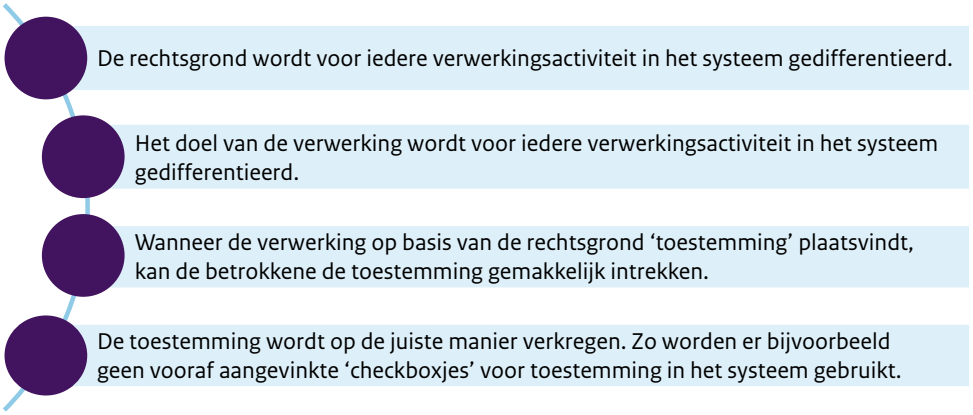
Persoonsgegevens mogen niet zomaar worden verwerkt. Iedere verwerking dient op een concrete (rechtmatige) grondslag gebaseerd te zijn: een rechtsgrond. Deze rechtsgronden zijn vertaald in artikel 6 AVG.[14]

**Rechtsgronden artikel 6 AVG**

- Gebaseerd op **toestemming** van betrokkene;
- Noodzakelijk is voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is;
- Noodzakelijk is om te voldoen aan een **wettelijke verplichting** van de verwerkingsverantwoordelijke;
- Noodzakelijk is ter **bescherming van vitale belangen**;
- Noodzakelijk voor de **vervulling van een taak van algemeen belang of openbaar gezag** door de verwerkingsverantwoordelijke;
- Noodzakelijk is voor de **behartiging van de gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde.

14 In de AVG zijn de zes (limitatieve) rechtsgronden neergelegd in artikel 6. Voor de verwerking van bijzondere categorieën van persoonsgegevens moet er – naast een grondslag uit artikel 6 AVG – een beroep kunnen worden gedaan op een van de uitzonderingen op het verbod om bijzondere categorieën van persoonsgegevens te verwerken die zijn neergelegd in artikel 9 lid 2 AVG. Een deel van die uitzonderingen uit artikel 9 lid 2 AVG is nader uitgewerkt in de Uitvoeringswet AVG (UAVG) of andere (sectorale) wetgeving.

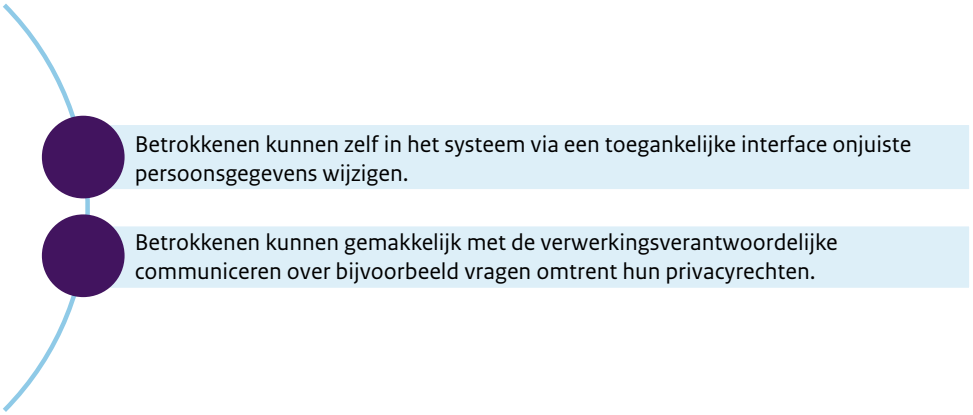
Belangrijke PbD elementen zijn onder meer:




Het **behoorlijkheidsprincipe** houdt in dat gegevensverwerkingen, naast rechtmatigheid, ook moeten voldoen aan de privacybeginselen uit artikel 5 AVG.

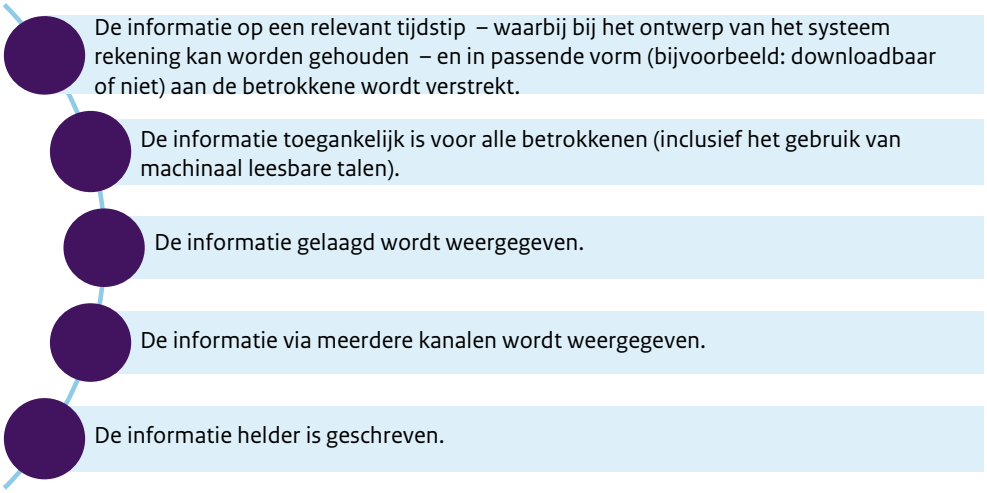
Zie voor achtergrondinformatie over de **verhouding tussen de privacybeginselen en PbD** paragraaf 4.2 van deze handleiding.

Belangrijke PbD elementen zijn onder meer:




Het **transparantieprincipe** ziet op de verplichting van verwerkingsverantwoordelijken om betrokkenen op de hoogte te stellen van het feit dat er een verwerking van zijn persoonsgegevens plaatsvindt en waarom. Het transparantiebeginsel is, naast artikel 5 AVG, nader uitgewerkt in artikelen 12-14 AVG.

Belangrijke PbD elementen zijn onder meer dat:




### 6.1.2. Doelbinding (artikel 5 lid 1 onder b AVG)

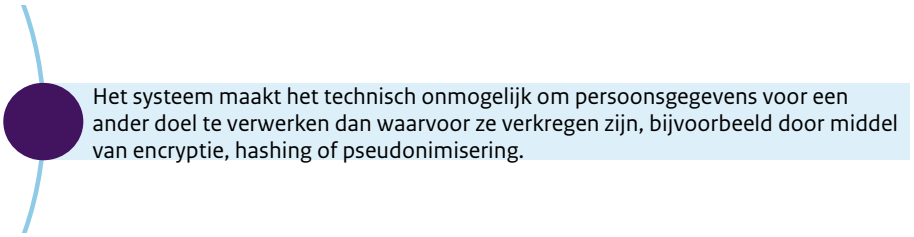
**Kern**: is de manier waarop ik de gegevensverwerking inricht zorgvuldig en behoorlijk zodat de uitvoer rechtmatig is en blijft?

Het **doelbindingsprincipe** bestaat uit de volgende twee onderdelen:

- Persoonsgegevens mogen niet worden gebruikt voor andere doelen dan waarvoor zij oorspronkelijk zijn verzameld; en
- Persoonsgegevens mogen wel worden gebruikt voor andere doelen dan waarvoor zij oorspronkelijk zijn verzameld wanneer deze nieuwe doelen verenigbaar zijn met het oorspronkelijke doel van verwerking.

Het ontwerp van de verwerking moet daarom worden vormgegeven op basis van wat noodzakelijk is om doeleinden te bereiken. Het doel van de verwerking stuurt het onderwerp en legt de grenzen daarvan vast. Ook dienen er maatregelen te worden genomen die ervoor zorgen dat gegevens niet (gemakkelijk) voor een ander doel kunnen worden hergebruikt.

Belangrijke PbD elementen zijn onder meer:



Bij de technische implementatie van doelbinding kunnen de volgende technische methoden helpen:

| | |
|---|---|
| **Technische implementatie** | Classificatie bronnen & labeling (zodat duidelijk is welke data het gaat zodat eenvoudiger de afweging kan worden gemaakt of het noodzakelijk is deze data te verwerken) |
| | Data classificatie & labeling (zodat duidelijk is welke data het gaat zodat eenvoudiger de afweging kan worden gemaakt of het noodzakelijk is deze data te verwerken) |
| | Data lineage (zodat men weet welke gegevens voor welk doel gebruikt worden) |

### 6.1.3. Minimale gegevensverwerking (artikel 5 lid 1 onder c AVG)

**Kern**: is de manier waarop ik de gegevensverwerking inricht zorgvuldig en behoorlijk zodat de uitvoer rechtmatig is en blijft?

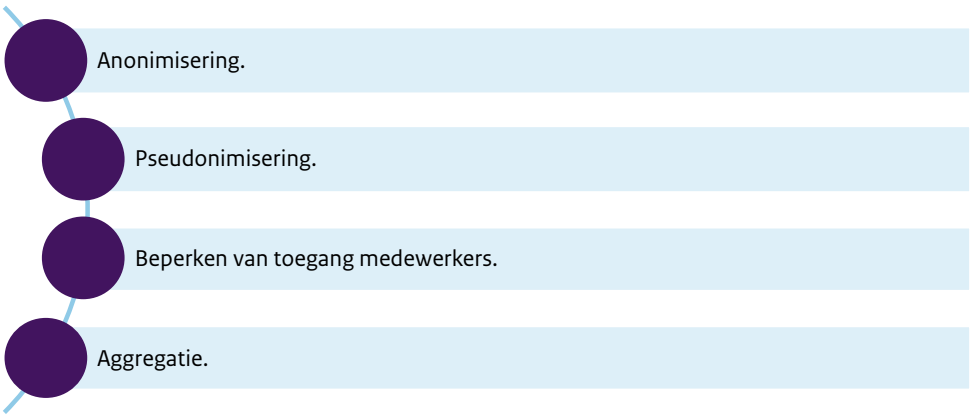
Het **data-minimalisatieprincipe** bestaat uit de volgende twee onderdelen:

- Er mogen niet meer persoonsgegevens worden verzameld dan noodzakelijk voor het bereiken van de doelen. Dit kan worden bereikt door na te denken over de doelomschrijving.

  Waarom worden deze gegevens verzameld? En zijn deze persoonsgegevens toereikend om de doelen te bereiken?

Het is hierbij van belang om zorgvuldig te kijken op welke manier(en) persoonsgegevens de organisatie binnenkomen en kritisch te bekijken of al die persoonsgegevens ook echt nodig zijn. Ook dient te worden nagegaan of er niet te veel persoonsgegevens met ketenpartners worden gedeeld.

Belangrijke PbD elementen zijn onder meer:



Bij de technische implementatie van minimale gegevensverwerking kunnen de volgende technische methoden helpen:

| | |
|---|---|
| **Technische implementatie** | Select before you collect (whitelisting) |
| | Exclude (blacklisting) |
| | Strip or destroy |
| | Anonimisering |

### 6.1.4 Juistheid (artikel 5 lid 1 onder d AVG)

**Kern**: is de manier waarop ik de gegevensverwerking inricht zorgvuldig en behoorlijk zodat de uitvoer rechtmatig is en blijft?

Het **juistheidsprincipe** bestaat uit de volgende twee onderdelen:

- De persoonsgegevens moeten juist en up-to-date zijn; en
- Er moet gehoor gegeven kunnen worden aan de rechten van betrokkenen.

Ten aanzien van het eerste bulletpoint kan worden gekeken naar de bronnen van de gegevens. Waar komen de persoonsgegevens vandaan en wat is de betrouwbaarheid van de bron. Verder kan ook worden gekeken naar de nauwkeurigheid van persoonsgegevens in verband met het doel waarvoor ze verzameld zijn. Tot slot kunnen vrije tekstvelden, webformulieren, documentatie, etc. worden aangepast zodat er minder kans is om foutieve persoonsgegevens te verzamelen en de kans op fouten wordt verkleind.

Bij de technische implementatie van juistheid kunnen de volgende technische methoden helpen:

| | |
|---|---|
| **Technische implementatie** | Controle op ETL processen, ETL auditing en unit testing |
| | Master data management (golden record betrokkene). Master data management bestaat naast specifieke technische tools voor een groot deel uit een organisatorische vaardigheid omtrent processen en afspraken en bijbehorende kennis en functionarissen. Vooral dat laatste kan in de praktijk lastig zijn |
| | Inrichting Crud |
| | Inrichten beperken persoonsgegevens, verwijdering, et cetera |
| | Inrichting controle betrokkenen (bijvoorbeeld via privacy portal) |

### 6.1.5. Opslagbeperking (artikel 5 lid 1 onder e AVG)

**Kern**: is de manier waarop ik de gegevensverwerking inricht zorgvuldig en behoorlijk zodat de uitvoer rechtmatig is en blijft?

Het **opslagbeperkingsprincipe** bestaat uit de volgende twee onderdelen:

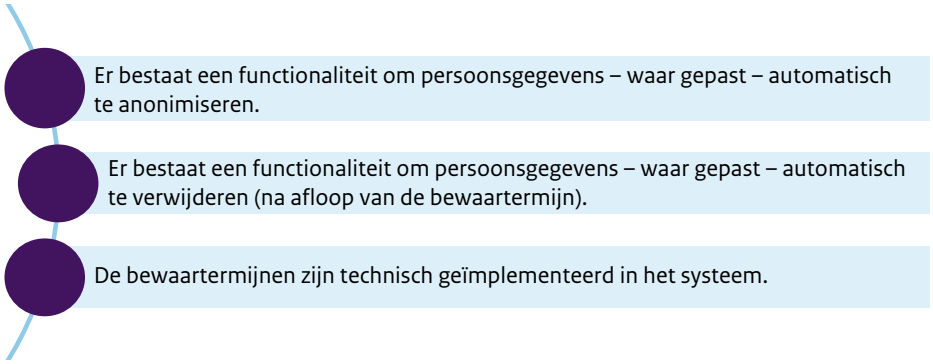
- De persoonsgegevens mogen niet langer bewaard worden dan nodig is om de doeleinden van de verwerking te bereiken (persoonsgegevens dienen daarna doeltreffend – en bij voorkeur automatisch - te worden verwijderd of geanonimiseerd); en

- De persoonsgegevens mogen wel langer bewaard worden wanneer dit verband houdt met archivering in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden, maar alleen als passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.

Sub-vragen die hierbij kunnen worden gesteld zijn:

- is het duidelijk welke persoonsgegevens voor welke periode moeten worden bewaard en waarom? Is dit in beleid neergelegd?
- is er bepaald welke persoonsgegevens nodig zijn voor back-ups en logbestanden? Is er bepaald welke bewaartermijn daarvoor geldt, en is die uitlegbaar?

Belangrijke PbD elementen zijn onder meer:




Bij de technische implementatie van opslagbeperking kunnen de volgende technische methoden helpen:

| | |
|---|---|
| **Technische implementatie** | Labeling data |
| | Geautomatiseerde inrichting verwijdering gegevens |
| | Inrichting privacy portal betrokkenen |

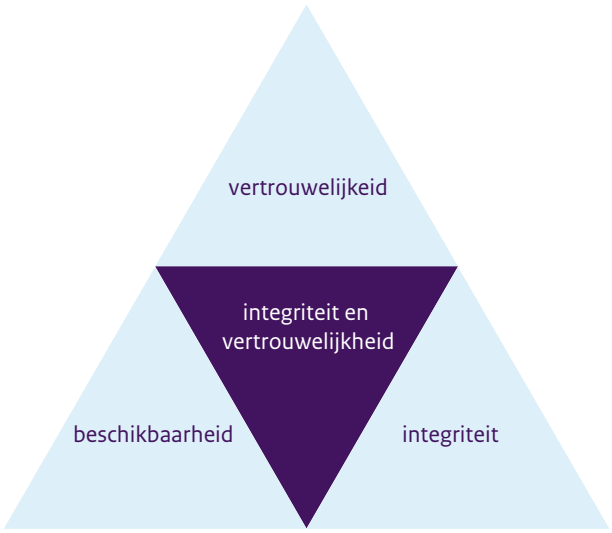
### 6.1.6. Integriteit en vertrouwelijkheid (artikel 5 lid 1 onder f AVG)

Kern: is de manier waarop ik de gegevensverwerking inricht zorgvuldig en behoorlijk zodat de uitvoer rechtmatig is en blijft?

De **integriteits- en vertrouwelijkheidsbeginselen** bestaat uit de volgende drie onderdelen (zie figuur 4.1):

- De persoonsgegevens moeten in vertrouwelijkheid verwerkt worden;
- De integriteit van de persoonsgegevens moet gewaarborgd worden; en
- De persoonsgegevens moeten beschikbaar zijn.

**Figuur 6.1.** Overzicht opbouw integriteits- en vertrouwelijkheidbeginsel.




Sub-vragen die hierbij kunnen worden gesteld zijn:

- is het duidelijk hoe op veiligheidsincidenten gereageerd moet worden? Zijn de routines, beleid, procedures en middelen in orde?
- hoe trekken we lering uit veiligheidsincidenten?
- is er voldoende contact tussen de privacy experts en de beveiligingsexperts?
- is er een onderscheid gemaakt tussen persoonsgegevens die beveiligd moeten worden overgedragen en waar dit niet noodzakelijk is?
- kunnen backups worden gepseudonimiseerd, bijvoorbeeld door hashing?

Belangrijke PbD elementen zijn onder meer:

- De organisatie beschikt over een *incident response plan*.
- Houd back-ups en logbestanden bij.

Bij de technische implementatie van integriteit en vertrouwelijkheid kunnen de volgende technische methoden helpen:

| | |
|---|---|
| **Technische implementatie** | Beperk/ reguleer toegang, bijvoorbeeld aan de hand van een autorisatiematrix (risico) |
| | Scherm af/ versleutel (encrypt) |
| | Pseudonimiseer, bijvoorbeeld door hashing |
| | Obfuscate (maak onbegrijpbaar) |
| | Beveilig de software/ persoonsgegevens |

Bij de implementatie van het integriteits- en vertrouwelijkheidsbeginsel is autorisatiebeheer belangrijk. Door middel van een autorisatiematrix kan grip worden gehouden op de toegang tot systemen en gegevens. Als er nog geen autorisatiematrix is opgesteld, dient deze te worden opgesteld. Let daarbij met name op de volgende punten:

- Inventariseer huidige informatiesystemen – en processen;
- Inventariseer gebruikersgroepen per informatiesysteem – en proces;
- Bepaal rechten voor gebruikersgroepen: leesrechten van gegevens, aanmaken van gegevens, verwijderen van gegevens, uitvoeren van specifieke functies, koppel rechten aan rollen, inventariseer speciale permissies.
- Stel een autorisatiematrix op.

### 6.1.7. Verantwoordingsplicht (artikel 5 lid 2 AVG)

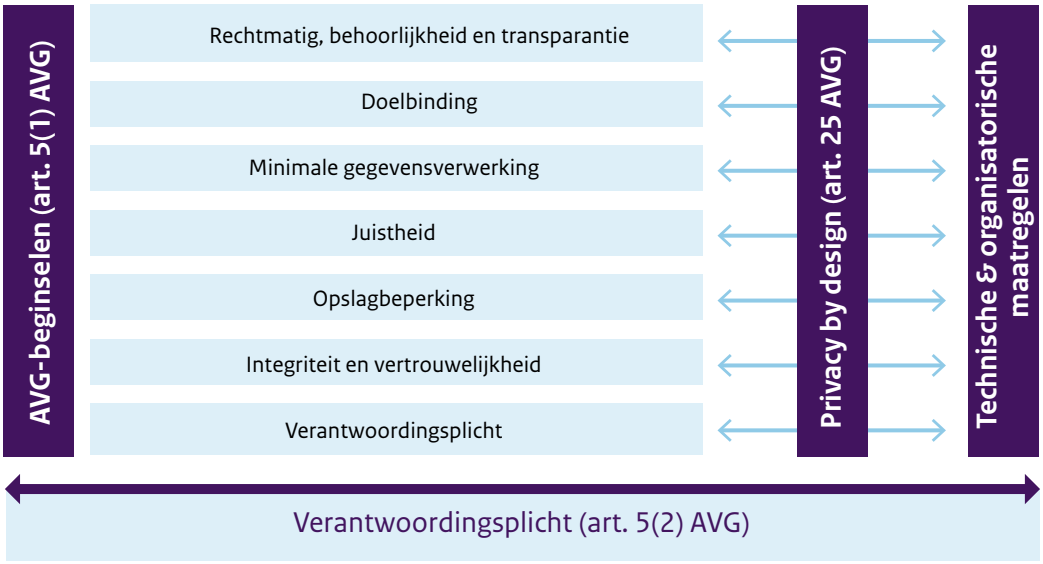
**Kern**: kan de verwerkingsverantwoordelijke aantonen dat bij het verwerken van persoonsgegevens wordt voldaan aan de privacybeginselen?

De verantwoordingsplicht is dat de verwerkingsverantwoordelijke moet kunnen aantonen dat aan alle beginselen hiervoor is voldaan.

Als de verwerkingsverantwoordelijke dit kan aantonen, betekent dit dat de verwerkingsverantwoordelijke ook al voor een belangrijk deel voldoet aan PbD.

Het beginsel van verantwoordingsplicht is daarbij overkoepelend (zie figuur 4.2): op grond van dit beginsel moet de verwerkingsverantwoordelijke verantwoordelijk zijn voor het kiezen van de noodzakelijke technische en organisatorische maatregelen ter bescherming van de rechten van de betrokkenen hebben en waarom zij passend en doeltreffend worden geacht en moet deze kunnen waarom zij passend en doeltreffend worden geacht.

**Figuur 6.2.** Verhouding PbD, verantwoordingsplicht en overige privacybeginselen.




## 6.2. Noodzakelijkheid

Wanneer een nieuw proces, applicatie of dienst wordt ontworpen waar persoonsgegevens een rol spelen, moet elke keer de vraag worden gesteld of het noodzakelijk is om bepaalde persoonsgegevens te verwerken.

De noodzakelijkheid is een belangrijk onderdeel van een 'goede' gegevensverwerking. De vraag die moet worden gesteld is of het werkelijk noodzakelijk is om het persoonsgegeven te verwerken voor het doel. De volgende vragen spelen hierbij een doorslaggevende rol:

- Is er een **objectieve reden** voor de verwerking?
- Staat het in verhouding tot het doel om dat persoonsgegeven te verwerken te verwerken (**proportionaliteit**)?
- Is het doel niet te bereiken zonder dat persoonsgegeven te verwerken (**subsidiariteit**)? Of misschien wel met minder persoonsgegevens?

# 7. Rollen bij PbD

**Tabel 7.1.** Rollen bij PbD.

| Rol | Taak i.k.v. PbD |
|---|---|
| **Bestuur, Directie** | Eindverantwoordelijke voor beleidsvorming, communicatie en uitvoering daarvan, het toewijzen van taken en rollen en evaluatie op basis van rapportages. |
| **Enterprise architect** | Helpen van de organisatie met het realiseren van de strategische doelstellingen en missie en visie. Hierdoor staat de Enterprise Architect niet alleen midden in de organisatie, maar neemt hij of zij ook alle externen mee, waaronder partners, leveranciers, klanten, overheid en wet- en regelgeving. |
| **Systeem architect** | Ontwerpen van het gehele systeem met alle IT-oplossingen voor een organisatie en daarbij kijken naar alle IT-componenten die met elkaar de IT en privacy behoeften van een organisatie afdekken. |
| **Solution architect** | Uitvragen privacy *requirements* bij het beleid en staf.<br>Analyseren privacy impact gekozen technologie solution/ stack.<br>Stroomlijnen *requirements* over *solutions* heen. |
| **Product managers, Developers** | Inschatten van privacy impact van *user stories* vanuit technisch perspectief. |
| **Beheerders** | Uitvragen privacy *requirements* bij het beleid en staf.<br>Beheer van privacy/ security binnen systemen. |
| **Testers, User acceptance** | Beoordeling systemen vanuit eindgebruikersperspectief. |
| **POs** | Toezichthouden op de omgang met persoonsgegevens, bekleden van een adviserende rol ten aanzien van privacy gerelateerde zaken en geven van trainingen om de interne kennis over privacy en gegevensbescherming te vergroten. |
| **FG** | Toezichthouden binnen de organisatie op de toepassing en naleving van de wetgeving rondom privacy en gegevensbescherming, waaronder de AVG. |
| **Chief Information Security Officer** | Verantwoordelijk voor informatiebeveiliging. |

# DEEL III | aanvullende bronnen en overzichten

## 8. Overzicht gebruikte tabellen in handleiding

| No. | Omschrijving |
|---|---|
| **2.1.** | PbD ontwerpstrategieën en tactieken. |
| **2.2.** | Ontwerpstrategieën in verhouding tot de privacybeginselen voor gegevensverwerking. |
| **3.1.** | Invulling passende maatregelen in verband met vertrouwelijkheid, integriteit en beschikbaarheid van informatie en systemen. |
| **3.2.** | Relevante componenten voor de inrichting van systemen en processen. |
| **3.3.** | Relevante vragen bij de inventarisatie van risico beperkende maatregelen gedurende de fasen van de levenscyclus van de verwerking. |
| **3.4.** | Toolkit implementatie PbD middels technische en organisatorische maatregelen. |
| **5.1.** | Aanvullende factoren bepaling 'passende technische en organisatorische maatregelen'. |
| **7.1.** | Rollen bij PbD. |

## 9. Overzicht gebruikte figuren in handleiding

| No. | Omschrijving |
|---|---|
| **2.1.** | Ontwerpstrategieën in de verhouding verwerkingsverantwoordelijke (data controller)-betrokkene (data subject). |
| **2.2.** | PbD data en proces georiënteerde ontwerpstrategieën. |
| **2.3.** | PbD beslisboom. |
| **3.1.** | Kwantificering risico. |
| **3.2.** | Componenten van gegevensverwerkingen binnen systemen en processen. |
| **3.3.** | Uitvoering DPIA in verband met PbD ontwerpstrategieën. |
| **3.4.** | Implementatie van PbD via AVG-beginselen, PbD ontwerpstrategieën en PET's. |
| **3.5.** | Project definiëring, risicobeoordeling en implementatie mitigerende maatregelen. |
| **4.1.** | AVG-normen, ontwerpstrategieën en PET's. |
| **5.1.** | De PbD-vuistregels. |
| **5.2.** | De implementatie van PbD gedurende de systeemlevenscyclus. |
| **6.1.** | Overzicht opbouw integriteits- en vertrouwelijkheidbeginsel. |
| **6.2.** | Verhouding PbD, verantwoordingsplicht en overige privacybeginselen. |

# 10. Overzicht achtergrondinformatie en aanvullingen

**Overzicht achtergrondinformatie:**

EDPB. (2020). Guidelines 4/2019on Article 25 Data Protection by Design and by Default. Online vindbaar via: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Schermer, B. W., & Toornstra, J. (2023). Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming. Online vindbaar via: https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming.

Hoepman, J. H. (2018). Privacyontwerpstrategieën (Het Blauwe Boekje). Online vindbaar via: https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf.

# 11. Bijlagen

### Bijlage A

Hieronder volgt een lijst met begrippen en afkortingen. Alle begrippen die in de AVG worden gedefinieerd, worden niet in onderstaande begrippenlijst gedefinieerd.

| Definitie | Beschrijving |
|---|---|
| Anonimisering | De AVG is van toepassing op de verwerking van persoonsgegevens, dat wil zeggen gegeven die betrekking hebben of een geïdentificeerde of identificeerbare natuurlijke persoon. Het is om deze reden dat de AVG en gerelateerde wetgeving inzake gegevenbescherming niet van toepassing zijn op anonieme gegevens, dat wil zeggen gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is (zie verder overweging 26 AVG).<br><br>In de praktijk kan het een uitdaging zijn om persoonsgegevens volledig te anonimiseren. Voor meer achtergrond kan worden gekeken naar publicaties / opinies van de EDPB en de voorloper van de EDPB, de Article 29 Data Protection Working Party. |
| AVG | Algemene verordening gegevensbescherming. |
| Behoorlijkheid | Een verwerking van persoonsgegevens is behoorlijk als deze rechtmatig is en er een objectieve rechtvaardigingsgrond (‘goede reden’ gebaseerd op feiten en de wet) is voor de verwerking. |
| Doelbinding | Persoonsgegevens mogen alleen voor de vooraf uitdrukkelijk en expliciet omschreven doeleinden worden verwerkt; (artikel 5 lid 1 b AVG). Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, moet beoordeeld worden of deze (nieuwe) verdere verwerking verenigbaar toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld; (artikel 6 lid 4 AVG). |
| DPIA | Data Protection Impact Assessment. Wordt ook wel aangeduid als gegevens-beschermingseffectbeoordeling (GEB). Dit betreft een instrument waarmee onderzoek gedaan kan worden naar de privacyrisico’s van de verwerking van persoonsgegevens. Een DPIA is in sommige gevallen verplicht; (artikel 35 AVG). |
| FG | Functionaris gegevensbescherming. |
| Grondslag | De AVG kent zes grondslagen: toestemming, uitvoering van de overeenkomst, wettelijke verplichting, vitaal belang van betrokkene of andere personen, algemeen belang of gerechtvaardigd belang. Op een van deze grondslagen moet de verwerking van persoonsgegevens gebaseerd zijn; (artikel 6 AVG). Als er sprake is van bijzondere persoonsgegevens moet daarnaast een grondslag worden gevonden in artikel 9 AVG. |
| Noodzakelijk | Omschreven in paragraaf 4.2. van deze handleiding. |

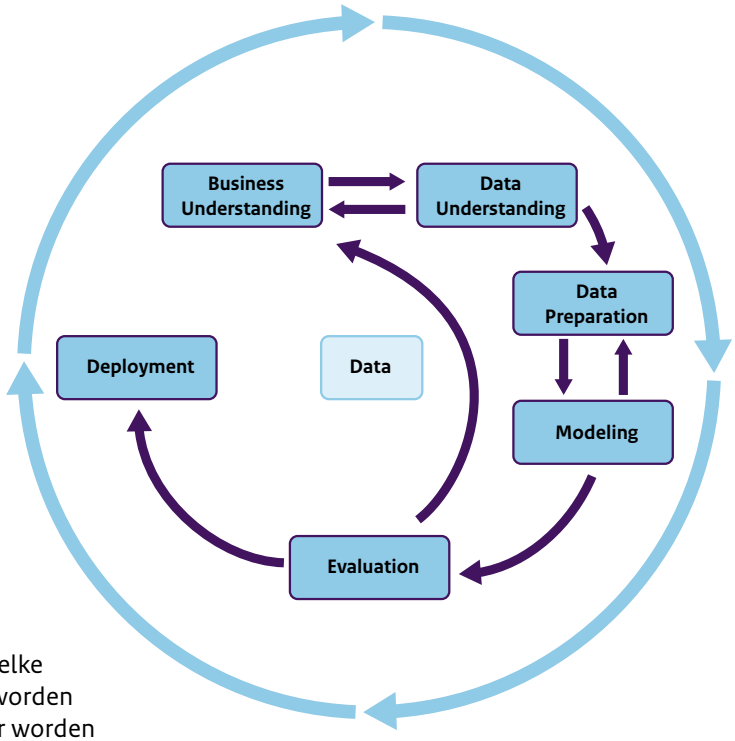
| Definitie | Beschrijving |
|---|---|
| Passende technische – en organisatorische maatregelen | De verwerkingsverantwoordelijke moet passende technische- en organisatorische maatregelen nemen om mogelijke risico's van de verwerking van persoonsgegevens te minimaliseren. Deze maatregelen zijn in overeenstemming is met de stand van de techniek. Daarbij zijn de maatregelen proportioneel met de hoogte van de risico's. Naarmate deze risico's groter zijn, worden zwaardere eisen gesteld aan de bescherming van de persoonsgegevens. Bij het bepalen van passende technische en organisatorische maatregelen wordt rekening gehouden met:<br>• de stand van de techniek die van toepassing zijn in het verwerkingsproces;<br>• de uitvoeringskosten;<br>• de aard, omvang, context en het doel van de verwerking; en<br>• de risico's voor de betrokkenen. |
| PO | Privacy officer |
| PDCA | Plan-Do-Check-Act |
| Privacy by Design (PbD) | Privacy by Design beoogt zo vroeg mogelijk in het ontwikkelingsproces van processen, (ICT-) producten en/ of diensten aandacht te hebben voor privacy en hieraan op een praktische wijze in de technologische infrastructuur en/of de (organisatorische) processen daaromheen invulling te geven (artikel 25 AVG en overweging 78 AVG). |
| Proportionaliteit | Bij de beoordeling van de proportionaliteit wordt bekeken of de verwerking van persoonsgegevens, en daarbij de inbreuk op de privacy van betrokkenen, in redelijke verhouding staat tot het te bereiken doel van de gegevensverwerking. |
| Rechtmatigheid | Een verwerking is rechtmatig wanneer deze gebaseerd kan worden op één van de grondslagen, zoals bijvoorbeeld een wettelijke verplichting of toestemming; (artikel 6 AVG). In het geval van bijzondere persoonsgegevens moet de verwerking daarnaast zijn gebaseerd op een van de grondslagen uit artikel 9 AVG. |
| Subsidiariteit | Bij subsidiariteit wordt bekeken of het doel van de verwerking van persoonsgegevens met minder ingrijpende middelen kunnen worden bereikt. |
| Transparantie beginsel | Transparantie houdt in dat het voor de betrokkene duidelijk is dat zijn persoonsgegevens worden verwerkt, waarom en door wie. De verwerkingsverantwoordelijke is verplicht de betrokkene hierover te informeren. |
| Wjsg | Wet justitiële en strafvorderlijke gegevens |
| Wpg | Wet politiegegevens |

## Bijlage B

Datawetenschap (data science) houdt zich bezig met het verkrijgen van inzichten uit data. Data, waaronder persoonsgegevens en niet-persoonsgegevens kunnen worden verstaan, is van groot belang voor bijna iedere organisatie.

In data science procedures wordt veelal gebruik gemaakt van de **CRoss Industry Standard Process for Data Mining (crisp-dm)** om data-gedreven wekzaamheden helder in kaart te brengen. Dit model kan ook een relevant stappenplan bieden voor de praktische implementatie van PbD, voornamelijk voor Data science teams.

Het crisp-dm model bestaat uit de volgende stappen:




- *Business understanding* – wat heeft de organisatie nodig? Binnen deze stap wordt het doel bepaald en de behoefte van de business in kaart te brengen. Wat moet het resultaat van een bepaald project zijn? Deze antwoorden zijn nodig om keuzes te maken en doelgerichtere analyses te doen.
- *Data understanding* – welke data hebben we beschikbaar en/of nodig? Is de data bruikbaar? Wat zegt deze data?
- *Data prepararation* – hoe wordt de data gestructureerd voorbereid voor analyse? Welke selecties kunnen er bijvoorbeeld gemaakt worden en hoe kan test- en trainingsdata van elkaar worden onderscheiden?
- *Modeling* – welke modelleringstechnieken moeten worden toegepast? Bij deze stap dienen de data te worden geselecteerd en het algoritme of de techniek om de computer het werk te laten doen.
- *Evaluation* – welke modellen beantwoorden het best aan de bedrijfsdoestellingen? Op basis van de scores wordt het beste model gekozen,
- *Deployment* – Inzet van het model.

## Bijlage C

Hieronder wordt een **risicobeoordelingsmatrix** weergegeven die inzicht biedt in de verhouding tussen kans en impact bij de afweging van privacy/ gegevensbeschermingsrisico's. Een risicomatrix kan per voorgenomen gegevensverwerking worden ingevuld. De cijfers in de risicobeoordelingsmatrix hieronder corresponderen met de voorbeelden die zijn weergegeven onder de matrix.

| | | **Kans dat het risico zich voordoet** | | | | |
|---|---|---|---|---|---|---|
| | | Zeer on-waarschijnlijk | Onwaar-schijnlijk | Mogelijk | Kansrijk | Zeer kansrijk |
| **Effect wanneer het risico zich voordoet** | Minimaal | Laag | Laag | Laag (voorbeeld 1) | Laag (voorbeeld 2) | Gemiddeld (voorbeeld 3) |
| | Licht | Laag | Laag | Gemiddeld | Gemiddeld (voorbeeld 4) | Gemiddeld |
| | Gemiddeld | Laag | Gemiddeld | Gemiddeld | Gemiddeld (voorbeeld 5) | Hoog (voorbeeld 6) |
| | Groot | Laag | Gemiddeld | Gemiddeld (voorbeeld 7) | Hoog (voorbeeld 8) | Hoog (voorbeeld 9) |
| | Zwaar | Gemiddeld (voorbeeld 10) | Gemiddeld (voorbeeld 11) | Hoog (voorbeeld 12) | Hoog (voorbeeld 13) | Hoog |

Let op: onderstaande voorbeelden zijn AVG-breed en niet alleen beperkt tot PbD.

| No. | Voorbeeld |
|---|---|
| 1 | Bij een verwerker werd er altijd vanuit gegaan dat de verwerkingen in Nederland plaatsvonden. Bij controle blijkt dat de verwerkingen in Frankrijk plaatsvinden. Het register, de verwerkingsovereenkomst en de privacyverklaring moeten worden aangepast. |
| 2 | Binnen een organisatie wordt per ongeluk een lijstje met een paar namen doorgemaild naar een verkeerde collega. |
| 3 | De thuiswerkomgeving voor medewerkers van de organisatie is niet bereikbaar voor de vierde keer in een week. |
| 4 | De website overheid.nl is een paar uur niet bereikbaar door een DDoS-aanval op die website. |
| 5 | Bij het invoeren van persoonsgegevens over een burger in een systeem, kan de medewerker van de overheid al beginnen met het invullen van het dossier, terwijl de gegevens nog niet volledig zijn uitgevraagd. Er gaat een hele tijd overheen voordat de aanvullende gegevens volgen. Er wordt niet meer gecontroleerd of de eerder ingevulde gegevens nog kloppen. |
| 6 | Er is geen adequaat proces ingeregeld voor betrokkenen om hun rechten te kunnen uitoefenen. Dat proces moet verbeterd worden. |
| 7 | Gegevens worden op basis van de selectielijsten bewaard. Niemand binnen de organisatie heeft zich ooit afgevraagd of alle gegevens moeten worden bewaard van deze burger en/ of sommige gegevens toch niet eerder verwijderd kunnen worden dan de selectielijst voorschrijft. |
| 8 | Een bepaalde verwerking komt (als categorie) voor op de lijst van de Autoriteit Persoons-gegevens waarvoor een DPIA moet worden uitgevoerd. Dit wordt over het hoofd gezien en de DPIA wordt pas veel later alsnog uitgevoerd. |
| 9 | Een medeweker van een organisatie is benieuwd of een vervelende buurman in een van de dossiers staat en gaat op zoek. De medewerker vindt en opent het dossier, terwijl de medewerker op grond van zijn functie dat dossier niet hoeft te raadplegen. |
| 10 | Er wordt een nieuwe leverancier gezocht voor een applicatie. Deze leverancier voldoet aan alle wensen en eisen uit het bestek. Een paar dagen na de gunning verschijnt in de media het bericht dat deze leverancier zeer corrupt is en samenwerkt met partijen waar de organisatie niet mee geassocieerd wil worden. |
| 11 | Een medewerker wil graag gegevens uit het dossier halen en dit thuis aan zijn partner laten zien. Het systeem is goed beveiligd, dus downloaden lukt niet. De medewerker heeft echter een achtergrond in software engineering en past een kunstgreep toe om de gegevens uit het systeem te halen. Hij neemt deze gegevens mee naar huis op een usb-stick. |
| 12 | Een DPIA uitvoeren is geen verplicht onderdeel van het proces. Een medewerker kan deze stap gemakkelijk overslaan zonder consequenties. De medewerker slaat deze stap over en meldt dat er geen privacy risico's zijn in dat proces. |
| 13 | Bij het ontwerp van een systeem is geen rekening gehouden met ethische aspecten van de gegevens die daarin worden verwerkt. Tijdens het uitvoeren van de DPIA wordt geconcludeerd dat er een risico kan bestaan op discriminatie door de voorgenomen gegevensverwerking. Het gaat veel tijd, energie en geld kosten om het systeem aan te passen. |

Een hulpmiddel voor het inschatten van een risico, is het vijf keer stellen van de **waarom vraag**, zoals ook het volgende voorbeeld illustreert:

Situatie: Er is een hoge kans dat binnen organisatie X meer persoonsgegevens worden verwerkt dan noodzakelijk.

| | |
|---|---|
| De organisatie verwerkt meer persoons-gegevens dan nodig. | **WAAROM?** |
| Omdat de doelen van de gegevens-verwerking zijn niet helder afgebakend. | **WAAROM NIET?** |
| Omdat er nooit een DPIA is gedaan voorafgaand aan de gegevensverwerking. | **WAAROM NIET?** |
| Omdat we geen budget en mensen beschikbaar hadden om de DPIA uit te voeren. | **WAAROM NIET?** (Hier is ruimte voor een alternatief, namelijk door meer budget en mensen beschikbaar te stellen). |
| Omdat we de noodzaak niet zagen. | **WAAROM NIET?** (Hier is ruimte voor een alternatief, namelijk door noodzaak te creëren). |
| Omdat we geen pre-DPIA hebben uitgevoerd. | **UITKOMST**: het belang van het uitvoeren van een (pre-)DPIA is onderschat. (Dit leidt tot aanpassing van de werkwijze). |

Juni 2023 | Publicatie-nr. 23403825