Ministerie van Justitie en Veiligheid

Aan de slag met Privacy by Design (PbD) en Privacy Enhancing Technologies (PETs)

Verdiepingshandleiding

Auteurs: Suzanne van Willige, Bart Schermer, Jaap-Henk Hoepman
Versie: 1.0
Datum: september 2024
Opdrachtgever: Ministerie van Justitie en Veiligheid
Contactpersoon: Pauline Verhaak, p.m.verhaak@minjenv.nl

Inhoud

1. Inleiding

In 2023 publiceerde het Ministerie van Justitie en Veiligheid de Handleiding Privacy by Design. De handleiding vormt een uitwerking van het Privacy beleidskader van de organisatie. Het doel van de handleiding is om handvatten te bieden voor het concreet toepassen van Privacy by Design (PbD). Bent u nog niet bekend met de handleiding, dan vindt u in bijlage 1 een korte samenvatting.

Dit document laat aan de hand van vier casussen zien hoe u PbD in de praktijk brengt. We doen dit door ontwerpkeuzes en privacyverbeterende technologieën toe te passen die een ontwerp privacyvriendelijk(er) maken.

Per casus worden de belangrijkste privacyrisico's geïdentificeerd en uitdagingen voor het ontwerp geformuleerd. Vervolgens worden oplossingen in het ontwerp voorgesteld die leiden tot een privacyvriendelijke(re) oplossing. De voorbeelden in de uitwerkingen dienen ter inspiratie en zijn niet de enige manier om PbD toe te passen.

Nota bene: het betreft fictieve casussen die zijn geïnspireerd op het werkveld van JenV. Ze vormen géén huidig of voorgenomen beleid. De genoemde casussen bevatten gevoelige aspecten. Hoewel privacyvriendelijke(re) keuzes gemaakt kunnen worden in het ontwerp, betekent dit niet dat de voorgenomen toepassing ook daadwerkelijk noodzakelijk of wenselijk is.

1.1. Leeswijzer

In hoofdstuk 2 laten wij aan de hand van vier casussen zien hoe u PbD in de praktijk brengt. Per casus worden de grootste privacyrisico's geïdentificeerd. Deze risico's stellen ons voor ontwerpuitdagingen: hoe kunnen we in het ontwerp privacyrisico's voorkomen of verkleinen?

Op basis van deze ontwerpuitdagingen worden ontwerpkeuzes gepresenteerd die voortvloeien uit de verschillende PbD strategieën (zie Handleiding Privacy by Design of bijlage 1). Denk hierbij bijvoorbeeld aan het verminderen van de gegevens die worden vastgelegd (minimaliseer) of het versleutelen van gegevens (verberg). Waar mogelijk beschrijven wij concrete technieken en toepassingen die de privacy helpen beschermen, zogenaamde Privacy Enhancing Technologies (PETs).

In hoofdstuk 3 geven wij een overzicht van alle PETs die relevant kunnen zijn voor de behandelde casussen. Deze PETs zijn ook buiten de context van de genoemde casus te gebruiken. De PETs zijn voorzien van een korte uitleg van hun werking en toepassing. Verder zijn bronnen opgenomen die voor de toepassing van de PET relevant zijn (denk bijvoorbeeld aan wetenschappelijke artikelen en verwijzingen naar toepassingen).

In hoofdstuk 4 tenslotte worden alle besproken ontwerpuitdagingen, privacyrisico's en oplossingen nog eens op een rij gezet. Dit overzicht kan bijvoorbeeld worden gebruikt om in DPIAs snel risico's en risicobeperkende maatregel te identificeren en beschrijven.

2. Privacy by design casussen

2.1. Een privacyvriendelijke manier om de rechten van betrokkenen te waarborgen

2.1.1. De casus

Burgers hebben recht op inzage in hun persoonsgegevens. Daarnaast hebben burgers ook recht op wijzigingen en verwijdering van hun gegevens wanneer de gegevens niet kloppen of onterecht worden verwerkt. Wanneer de burger succesvol een wijzigings- of verwijderverzoek doet, dan moeten organisaties aan wie de gegevens zijn verstrekt hiervan op de hoogte worden gebracht.

Voor een organisatie kan dit het volgende betekenen:

Een betrokkene doet een inzageverzoek bij (een onderdeel van) de organisatie. Om invulling te geven aan dit verzoek moet onderzocht worden waar binnen de organisatie allemaal persoonsgegevens worden verwerkt van deze persoon. Vervolgens moet de organisatie terugkoppelen om welke gegevens het gaat en wat de doelen zijn waarvoor deze gegevens worden verwerkt. Inzageverzoeken worden door overheidsorganisaties vaak handmatig afgehandeld, met als gevolg dat het enige tijd duurt voordat een burger een reactie op een inzageverzoek ontvangt. Ook zijn handmatige processen doorgaans foutgevoeliger en kostbaarder. Het inzageproces kan worden gedigitaliseerd en geautomatiseerd om dit proces privacyvriendelijker te laten verlopen én afhandeling van verzoeken te versnellen. Hierdoor houden medewerkers meer tijd over voor maatwerk en het waarborgen van de menselijke maat in het contact met burgers.

2.1.2. Privacyrisico's en ontwerpuitdagingen

Op basis van deze casus kunnen we de volgende privacyrisico's identificeren en daaruit de bijbehorende ontwerpuitdagingen afleiden.

2.1.2.1. Identificatie

2.1.2.1.1. *Privacyrisico*

Om een inzageverzoek te kunnen behandelen moet de identiteit van de betrokkene met voldoende zekerheid kunnen worden vastgesteld. Gebeurt dit niet, dan eindigen de persoonsgegevens mogelijk bij onbevoegden. De organisatie kan twijfelen over de identiteit van een betrokkene als zij een verzoek doen. Indien dit het geval is, dan kan de organisatie aanvullende informatie vragen om de identiteit van de betrokkene te verifiëren.[1] Om zich te identificeren moet de betrokkene vervolgens (gevoelige) gegevens delen met de organisatie. Wanneer (teveel) gegevens worden gedeeld dan levert dit een privacyrisico op voor de betrokkene. De opslag van deze gegevens kan ook het risico op datalekken vergroten wanneer bijvoorbeeld sprake is van een handmatig proces waarbij iemand een kopie paspoort opslaat in de email of op de eigen harde schijf.

2.1.2.1.2. *Ontwerpuitdaging*

De ontwerpuitdaging is om ervoor te zorgen dat er geen of zo min mogelijk gegevens gedeeld hoeven te worden tussen de betrokkenen en de organisatie, maar dat tegelijkertijd de organisatie de identiteit van betrokkene met voldoende mate van zekerheid kan vaststellen.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in paragraaf 2.1.3.1.

1 Zie artikel 12 lid 6 AVG

2.1.2.2. Correcte en integere afhandeling

2.1.2.2.1. *Privacyrisico*
Wanneer het verzoek ontvangen is en de identiteit van de betrokkene vastgesteld is, moet binnen de organisatie worden gezocht welke gegevens er allemaal beschikbaar zijn. Dat gebeurt binnen de meeste organisaties nog handmatig. Dit proces is niet alleen tijdrovend, maar het is ook foutgevoelig. Handmatige afhandeling van inzageverzoeken vormt daarmee een privacyrisico.

2.1.2.2.2. *Ontwerpuitdaging*
De uitdaging is om de gegevens van een persoon geautomatiseerd bij elkaar te kunnen brengen. Hiervoor is het noodzakelijk dat gegevens duurzaam aan de betrokkene zijn gekoppeld zelfs over of tussen verschillende systemen.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.1.3.2.

2.1.2.3. Uitwisseling gegevens tussen organisaties

2.1.2.3.1. *Privacyrisico*
Wanneer gegevens zijn gedeeld, dan moet het voor de betrokkene duidelijk zijn met wie. Ook voor het informeren van derden over wijzigings- en verwijderverzoeken moet bekend zijn welke derden de gegevens hebben gekregen. Wanneer er twijfel bestaat over met welke partijen allemaal gegeven zijn gedeeld, dan moet bij de potentiële ontvangers gecontroleerd worden of de betrokkene bij deze ontvanger bekend is (matching) en of de gegevens daadwerkelijk bij de organisatie vandaan komen. Hiertoe moet informatie van de betrokkene worden gedeeld met deze derde partijen. Dit vormt een privacyrisico, omdat de derde partijen mogelijk onbevoegd kennisnemen van persoonsgegevens van de betrokkene.

2.1.2.3.2. *Ontwerpuitdaging*
De uitdaging is om van een andere organisatie te weten te komen of gegevens zijn gedeeld met deze organisatie, zonder (te veel) identificerende gegevens van de betrokkene te delen met deze organisatie.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.1.3.3.

2.1.2.4. Veilige inzage geven

2.1.2.4.1. *Privacyrisico*
Voor de afhandeling van inzageverzoeken kunnen onbedoeld onveilige kanalen worden gebruikt. Wanneer het inzageverzoek van de burger bijvoorbeeld wordt afgehandeld via e-mail loopt de betrokkene het risico dat de gegevens onderweg worden afgevangen, omdat e-mail een onbeveiligd kanaal is. Datzelfde geldt voor het terugsturen van gegevens aan de betrokkene. Ook zorgt het gebruik van verschillende kanalen ervoor dat de gegevens minder goed te beheren zijn omdat ze op allerlei plekken (tijdelijk) opgeslagen worden.

2.1.2.4.2. *Ontwerpuitdaging*
De ontwerpuitdaging is om een gebruiksvriendelijk, maar veilig kanaal te creëren voor het versturen van de gegevens.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.1.3.4 en 2.1.3.5.

2.1.2.5. Volledigheid gegevens

2.1.2.5.1. *Privacyrisico*

Wanneer een verzoek tot inzage wordt gedaan, is het van belang dat de organisatie weet welke gegevens op een inzageverzoek van toepassing zijn. Allereerst moet een antwoord op een verzoek compleet zijn: de organisatie moet dus alle relevante gegevens tonen aan de betrokkene. Verder is het recht op inzage geen absoluut recht. Er kunnen redenen zijn om betrokkenen geen of gedeeltelijke inzage te geven in hun gegevens.

2.1.2.5.2. *Ontwerpuitdaging*

De uitdaging is om geautomatiseerd te bepalen welke gegevens wel of niet persoonsgegevens zijn en vervolgens welke van deze gegevens bij een inzage, correctie of verwijderingsverzoek betrokken moeten worden.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.1.3.2 en 2.1.3.5.

2.1.3. Oplossingen in het ontwerp

Aan de hand van de ontwerpstrategieën kan voor deze casus aan de volgende ontwerpkeuzes worden gedacht:

2.1.3.1. Gebruik sterke vormen van identificatie en authenticatie (verberg)

Sterke vormen van het identificatie en authenticatie kunnen helpen om de privacy van betrokkenen die een verzoek indienen beter te beschermen, zeker als de overheid zelf niet zomaar in staat is om gegevens in verschillende bestanden aan elkaar te koppelen.

Een voorbeeld van een sterke vorm van identificatie is het gebruik van DigiD. Als deelbestanden aan elkaar gekoppeld moeten worden, maar geen gebruik gemaakt is van het BSN (welke door DigiD betrouwbaar wordt geverifieerd), kunnen additionele gegevens voor nadere identificatie noodzakelijk zijn. Dit kan bijvoorbeeld door gebruik te maken van self-sovereign identity/attribuut gebaseerde credentials oplossingen zoals Yivi of de toekomstige Europese eID wallets, zie hiervoor paragraaf 2.1.3.6 en hoofdstuk 3.

2.1.3.2. Label gegevens als zijnde persoonsgegevens (dwing af)

Om (geautomatiseerd) invulling te kunnen geven aan de rechten van betrokkenen moet duidelijk zijn welke gegevens persoonsgegevens zijn (alleen of in hun onderlinge samenhang), wat het doel is voor hun verwerking en op welke juridische grondslag dat doel gebaseerd is. Door gegevens te labelen als persoonsgegevens kunnen deze automatisch herkend worden. Hierdoor hoeft er niet meer handmatig te worden gezocht naar de persoonsgegevens en telkens opnieuw beoordeeld te worden of het (relevante) persoonsgegevens zijn.

Data labeling stelt de organisatie vervolgens in staat om beleid (*business rules*) te koppelen aan de gegevens. Zo kan bijvoorbeeld de labeling gekoppeld worden aan de autorisatie van medewerkers. Op deze manier wordt voorkomen dat onbevoegde medewerkers toegang krijgen tot deze gegevens. Ook kan bij iedere verwerking automatisch gecontroleerd worden of deze verwerking op een specifiek persoonsgegeven toegestaan is, gezien het gelabelde doel en grondslag. De labels kunnen ook gebruikt worden bij de beoordeling of de gegevens relevant zijn voor een inzageverzoek.

Door middel van data labeling wordt er bij de ontvangst van persoonsgegevens van bijvoorbeeld burgers al onderscheid gemaakt tussen de verschillende type gegevens. Als er met een standaard aantal labels gewerkt wordt die vervolgens op een standaard locatie (beveiligd) opgeslagen worden, kan gegarandeerd worden dat alle relevante persoonsgegevens meegenomen worden bij een inzageverzoek. Toegang tot de

gegevens zelf is niet noodzakelijk, zolang de labels zichtbaar zijn die aan de gegevens hangen , waardoor de privacy officer kan afleiden dat deze onder het inzageverzoek vallen.

Een voorbeeld om data te labelen voor het uitvoeren van verzoeken voor de rechten van betrokkenen is Adobe's *Labeling Analytics data for privacy requests*.[2]

2.1.3.3. Matching technologie (scheid)

Om het probleem op te lossen dat te veel gegevens worden gedeeld tijdens het raadplegen of informeren van andere organisaties kan gebruik worden gemaakt van matching technologie. Een privacy officer kan in plaats van handmatig inzageverzoeken behandelen, met behulp van matchingstechnologie (zoals bijvoorbeeld Ma3tch) namen op het verzoek van burgers vergelijken (matchen).[3] Dit kan de privacy officer doen met een beperkt aantal gegevens die voor de privacy officer noodzakelijk zijn om de betrokkene te identificeren, waardoor overbodige gegevens over een persoon niet worden verwerkt. Op deze manier komt, naast de privacy officer, niemand binnen de organisatie de naam van de betrokkene te weten wanneer deze persoon niet bekend is bij de bevraagde overheidsorganisatie. Wanneer iemand voorkomt in de overheidsadministratie (sprake is van een 'hit') verzorgt de privacy officer het verificatieproces en kan deze door de snelheid van de decentrale techniek die wordt gebruikt zowel de 'hits' als 'no hits' versneld afhandelen.

2.1.3.4. Encryptie en pseudonimisering (verberg)

Om veilige inzage mogelijk te maken kan encryptie worden gebruikt. Door de gegevens versleuteld op te slaan en te versturen wordt voorkomen dat onbevoegde derden toegang krijgen tot de gegevens. Een andere mogelijkheid is om niet de gegevens zelf, maar een link naar de gegevens op een beveiligd webportaal te versturen (zie ook 2.1.3.5).

Bij het delen van gegevens met derden moet nagedacht worden over de vraag of de gegevens niet (deels) afgeschermd moeten worden. Door middel van pseudonimisering kunnen alleen de relevante gegevens worden gedeeld zonder dat de identificerende gegevens bekend worden. Het is zelfs mogelijk om een onderscheid te maken tussen verschillende ontvangers met behulp van polymorfe pseudonimisering.[4]

2.1.3.5. Proactief delen van informatie met de burger (informeer en controleer)

Een effectieve manier om privacyrisico's te verkleinen, is om te zorgen dat er minder inzageverzoeken hoeven te worden gedaan. Een manier om het aantal inzageverzoeken terug te dringen is de burger proactief informeren. Dit verkleint de kans op inzageverzoeken, omdat de burger al over de benodigde informatie beschikt. De burger kan bijvoorbeeld informatie verstrekt krijgen in de vorm van een dashboard of 'mijn' omgeving waarbinnen te zien is welke gegevens worden verwerkt. Omdat dit soort omgevingen makkelijker te beveiligen is, worden de problemen van onbeveiligde kanalen zoals email ook voorkomen.

2.1.3.6. Kies voor decentrale opslag bij de burger (scheid)

Veel van de privacyrisico's en ontwerpuitdagingen in deze casus kunnen worden voorkomen door zelf geen gegevens te verzamelen en op te slaan, maar de gegevens bij de burger te laten. Uiteraard hangt het af van de toepassing of het wenselijk is dat de burger volledige controle heeft over de gegevens (en bijvoorbeeld de overheid de toegang daartoe kan ontzeggen), maar voor de situaties waar het niet noodzakelijk is om als overheid zelf (exclusief) te beschikken over de gegevens, is dit een privacyvriendelijke oplossing. Wanneer

2 https://experienceleague.adobe.com/docs/platform-learn/tutorials/privacy/privacy-labels-in-adobe-analytics.html?lang=en.

3 Zie: https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2021/13/reportage-ma3tch.

4 Zie Hoofdstuk 7.

de burger zelf de beschikking heeft over zijn gegevens is er ook geen noodzaak meer tot het doen van inzageverzoeken.[5]

Burgers kunnen gegevens opslaan in een digitale kluis of portemonnee (personal data store of wallet). Uiteraard vormt de betrouwbaarheid van de inhoud van deze data store altijd een punt van aandacht. Wanneer bijvoorbeeld een burger moet bewijzen dat hij of zij boven de 18 is, dan kan dit op basis van zelfverklaring, maar wanneer er meer zekerheid nodig is dan kan er ook gewerkt worden met *trusted third parties* (zoals bijvoorbeeld een notaris) die instaan voor de waarachtigheid van de gegevens die in de personal data store opgeslagen zijn.

Een voorbeeld van een personal data store is Qiy.

2.2. Delen van gegevens binnen samenwerkingen

2.2.1. De casus

Een veiligheidshuis wil gegevens kunnen delen tussen verschillende ketenpartners (politie, OM, gemeente, GGZ, GGD, 3RO et cetera). De partijen willen specifieke informatie over een individu kunnen combineren, maar ook meer geaggregeerde inzichten krijgen, bijvoorbeeld om te kunnen onderzoeken of er een verband is tussen problematische schulden en huiselijk geweld. Zij weten van elkaar niet wie gegevens heeft over de betrokkene en waarom iemand geregistreerd staat in de systemen van een andere ketenpartner. De partners bevragen elkaar door eerst de identificerende gegevens van de betrokkene te delen met de andere ketenpartners ('dat' informatie) om zo te kunnen 'matchen' of beide partijen bekend zijn met de betrokkene. Wanneer er een 'hit' is, dan worden de onderliggende gegevens gedeeld ('wat' informatie).

2.2.2. Privacyrisico's en ontwerpuitdagingen

Op basis van deze casus kunnen we de volgende privacyrisico's identificeren en daaruit de bijbehorende ontwerpuitdagingen afleiden.

2.2.2.1. Delen 'dat' informatie

2.2.2.1.1. *Privacyrisico*

Het voornaamste risico van het delen van 'dat' informatie is dat gegevens van een betrokkene tussen organisaties worden gedeeld. Stel dat organisatie A wil weten of organisatie B gegevens heeft betreffende persoon X. Om vast te stellen dat persoon X bij organisatie B bekend is, zal organisatie A aan organisatie B bekend moeten maken dat zij op zoek is naar informatie over persoon X. Afhankelijk van de wijze waarop de matching tot stand wordt gebracht, kunnen gevoelige gegevens zoals bijvoorbeeld BSN, namen, geboortedatum et cetera gedeeld worden met organisatie B. Echter, er is geen garantie dat organisatie B überhaupt persoon X kent en/of de gebruikte 'dat' informatie mag verwerken. Daarnaast kan het simpele feit dat X bij A bekend is al een privacyrisico opleveren als dat bij navraag met B gedeeld wordt (en andersom, zie onder).

2.2.2.1.2. *Ontwerpuitdaging*

De ontwerpuitdaging is om te weten te komen of er een match bestaat tussen de datasets van twee organisaties, zonder dat de organisaties (te veel) informatie prijsgeven over hun dataset. Zowel bij het uitvragen als het ontvangen van gegevens. In de informatica staat dit probleem bekend als het 'private set intersection probleem'. [6]

5 Wanneer de overheid gegevens genereert die ook van belang zijn voor de burger, dan moet ook worden nagedacht over hoe deze in de personal data store van de burger komen.

6 M. Freedman, K. Nissim, and B. Pinkas. "Efficient private matching and set intersection". In: EUROCRYPT 2004 (Interlaken, Switzerland, May

De gewenste situatie is dat de vragende en de bevraagde partij enkel en alleen iets te weten komen als er een match is, en je wilt bovendien voorkomen dat een vragende partij A een vraag over persoon X kan stellen als X niet in de database van A zelf voor komt.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.3.3.1.

Nota bene: het matchen van 'dat' informatie tussen organisaties vormt eigenlijk altijd een privacyrisico. Een 'hit' betekent namelijk dat de organisatie die bevraagd wordt prijsgeeft dat zij de betrokkene in haar systemen heeft staan. Hieruit kan al gevoelige informatie worden afgeleid. Om die reden moet terughoudend worden omgegaan met matching, zelfs als dit op een privacyvriendelijke wijze gebeurt.

2.2.2.2. Delen 'wat' informatie

2.2.2.2.1. *Privacyrisico*

Bij het delen van inhoudelijke informatie ('wat' informatie) is het belangrijkste privacyrisico dat er zonder grondslag gegevens worden gedeeld. Met andere woorden, mag de organisatie die een andere organisatie bevraagt de gegevens wel hebben? En zo ja, worden niet te veel gegevens gedeeld? Op het moment dat er gegevensuitwisseling plaatsvindt tussen de verschillende partijen, bestaat er een kans dat er (ongevraagd) te veel informatie wordt gedeeld met de andere partij. Dit is vooral een risico op het moment dat er één grote uitwisseling van gegevens wordt uitgevoerd, en een uitwisseling niet in fases gebeurt of er geen deelvragen worden gehanteerd.

2.2.2.2.2. *Ontwerpuitdaging*

De ontwerpuitdaging is om een systeem te creëren dat geen of zo min mogelijk informatie prijsgeeft over betrokkenen. Zowel bij het uitvragen als het ontvangen van gegevens.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.3.3.5.

2.2.2.3. Beveiliging

2.2.2.3.1. *Privacyrisico*

Naast het onbevoegd vragen en/of ontvangen van gegevens is een bijkomend risico de beveiliging van de gegevens, maar ook de integriteit daarvan. Wanneer de verbindingen niet goed zijn beveiligd, dan kunnen gegevens bijvoorbeeld tijdens het transport worden afgevangen. Wanneer de gegevens die worden doorgegeven niet veilig worden opgeslagen, dan creëert dit ook een privacyrisico. Dit is met name een risico wanneer de gegevens 'handmatig' worden gedeeld (bijvoorbeeld Excel sheets met persoonsgegevens die via de email worden gedeeld).

2.2.2.3.2. *Ontwerpuitdaging*

De ontwerpuitdaging is om een systeem te creëren dat de vertrouwelijkheid en de integriteit van de gegevens garandeert.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.2.3.1.

2.2.2.4. Statistiek en analyse

2.2.2.4.1. *Privacyrisico*

In sommige gevallen is een vragende partij alleen geïnteresseerd in een statistiek over personen waarvan de data bij verschillende ketenpartners staat opgeslagen. Een voorbeeld van zo'n statistiek is: "Hoeveel cliënten van de reclassering staan op dit moment onder behandeling van een psychiater?" Door alle 'microdata' die nodig is om die statistiek te berekenen tijdelijk bij één partij te verzamelen voor de berekening, krijgt die partij toegang tot veel privacygevoelige gegevens.

2– 6, 2004). LNCS 3027. Springer, 2004, pp. 1–19.

Een ander privacyrisico rondom analyse is dat op basis van additionele gegevens, alsnog relevante informatie over één individu uit de statistiek kan worden herleid. Bijvoorbeeld omdat de groep personen waarover de statistiek berekend wordt te klein is om anonimiteit te garanderen. Hierdoor zou een ketenpartner de conclusie kunnen trekken dat een bepaalde cliënt hoogstwaarschijnlijk onder behandeling van een psychiater staat.

2.2.2.4.2. *Ontwerpuitdaging*
De ontwerpuitdaging is om een systeem te ontwerpen dat op een geaggregeerd niveau antwoord kan geven zonder dat de onderliggende persoonsgegevens allemaal voor één partij toegankelijk worden en/of de geaggregeerde uitkomsten alsnog gerelateerd kunnen worden aan een individu.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.2.3.2.

2.2.2.5. Bewaartermijnen

2.2.2.5.1. *Privacyrisico*
Als er gegevensuitwisseling plaatsvindt tussen verschillende partijen, worden de gegevens waarschijnlijk op verschillende plekken verwerkt en/of opgeslagen. Omdat persoonsgegevens een bepaalde bewaartermijn hebben, is er een risico dat bij de uitwisseling deze bewaartermijn verandert / niet meegenomen wordt en dat de gegevens langer bewaard blijven dan noodzakelijk. Ook is er een risico dat gegevens bij de ene partij verwijderd worden, maar bij de ander bewaard blijven terwijl dit niet de bedoeling is.

2.2.2.5.2. *Ontwerpuitdaging*
De uitdaging is om een systeem te ontwerpen waarbij bewaartermijnen worden ‘overgeërfd’ en/of geautomatiseerd afgedwongen worden. Of om een systeem te ontwerpen waarbij niet de data zelf gedeeld wordt, maar enkel (tijdelijk) toegang tot de data wordt gegeven bij de oorspronkelijke bron.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.2.3.5 en 2.2.3.6.

2.2.2.6. Verdere doorgifte

2.2.2.6.1. *Privacyrisico*
Tenslotte is er het vraagstuk van de verdere doorgifte van de gegevens. Zo kan een organisatie het goed vinden dat bepaalde gegevens worden doorgegeven aan organisatie A, maar er een probleem mee hebben als organisatie A deze gegevens vervolgens deelt met organisatie B.

2.2.2.6.2. *Ontwerpuitdaging*
De ontwerpuitdaging is om ervoor te zorgen dat de gegevens niet zonder meer verder gedeeld kunnen worden en de originele verstrekker een zekere mate van controle houdt over de verstrekte gegevens.

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.2.3.4, 2.2.3.5 en 2.2.3.6.

2.2.3. Oplossingen in het ontwerp

Aan de hand van de ontwerpstrategieën kan voor deze casus aan de volgende ontwerpkeuzes worden gedacht:

2.2.3.1. Matching technologie (scheid/verberg)

Ook in deze casus kan matching technologie gebruikt worden om de privacyrisico's te beheersen bij het delen van ‘dat’ informatie. In plaats van de volledige identificerende gegevens te delen met de ketenpartners om te bepalen of bepaalde personen ook bekend zijn bij organisatie B, worden de persoonsgegevens van deze groep personen gecodeerd. Deze codering is specifiek ontworpen om ervoor

te zorgen dat deze niet te herleiden is tot de personen zelf, terwijl toch op basis van deze gecodeerde gegevens beslist kan worden of een persoon X in deze gecodeerde verzameling voorkomt. De gecodeerde vraag kan dan aan organisatie B gestuurd worden, die vervolgens voor elk van de personen in de eigen bestanden kijkt of er een match is met de gecodeerde vraag. Elke match wordt als antwoord teruggestuurd. Deze matching is een vorm van secure multi-party computation, meer specifiek *private set intersection*. Een voorbeeld hiervan is Ma3tch, ontwikkeld binnen JenV en het FCInet Secretariaat.

2.2.3.2. Verkrijgen geaggregeerde inzichten (scheid/verberg, aggregeer)

Om op een privacyvriendelijke manier geaggregeerde inzichten te verkrijgen kan secure multi-party computation worden gebruikt. Met behulp van secure multi-party computation kan een willekeurige functie over een aantal verspreide databases worden berekend, zonder dat deze met anderen gedeeld hoeven te worden. Bijvoorbeeld om te bepalen of persoon X schulden heeft die groter zijn dan zijn of haar inkomen. In dit geval heeft de functie als invoer het inkomen zoals bekend bij de belastingdienst en de schulden zoals bekend bij het BKR, die dus berekend kan worden zonder dat het inkomen of de schuld met een willekeurige partij gedeeld hoeft te worden.

Een andere techniek is homomorfe encryptie, die het ook mogelijk maakt om te rekenen met versleutelde data. Tenslotte zijn er technieken zoals differential privacy[7] en statistical disclosure control[8] die ervoor kunnen zorgen dat een geaggregeerde statistiek geen informatie over de onderliggende microdata lekt. Deze technieken worden onder andere door het CBS gebruikt.

2.2.3.3. (Polymorfe) Pseudonimisering (scheid/verberg)

Een andere manier om de privacyrisico's te beheersen bij 'delen dat' is het gebruik van zogenaamde polymorfe pseudoniemen.[9] De achterliggende gedachte bij deze methode is dat personen voor iedere organisatie een apart, onderling niet zonder meer koppelbaar, pseudoniem hebben dat cryptografisch uit hun persoonsgegevens (bijvoorbeeld het BSN) wordt gegenereerd. Het pseudoniem voor persoon X bij organisatie A is dan ‘PseudoID(X,A)', terwijl het voor organisatie B ‘PseudoID(X,B) is. Gegevens die A over deze persoon beheert, worden onder dit pseudoniem bewaard. Zoals gezegd zijn de pseudoniemen van X bij verschillende organisaties A en B niet zondermeer koppelbaar. Om ervoor te zorgen dat de gegevens waar nodig toch aan elkaar gerelateerd kunnen worden is een aparte vertrouwde entiteit (de 'Transcriptor') noodzakelijk die deze koppeling wel kan maken: gegeven PseudoID(X,A) kan deze transcriptor PseudoID(X,B) berekenen. In het proces van 'delen dat' stuurt A de bij haar bekende pseudoniemen op aan de transcriptor, die deze vertaalt naar de pseudoniemen voor deze personen bij B, om vervolgens het al dan niet voorkomen van relevante gegevens voor deze pseudoniemen bij B uit te vragen.

2.2.3.4. Remote access (scheid/verberg)

Een andere mogelijke oplossing is het gebruik van remote access. Nadat bepaald is dat een ketenpartij (relevante) informatie over een persoon heeft, kan ervoor gekozen worden om niet een kopie van de data op te sturen naar de vragende partij, maar in plaats daarvan enkel remote access ("toegang op afstand") tot de relevante informatie te geven aan de vragende partij. De vragende partij krijgt een verwijzing naar de data opgestuurd, waarmee deze op afstand toegang kan verkrijgen tot de brondata bij de ketenpartij. De link geeft enkel toegang tot die data die relevant is, en voor zolang als toegang tot die data relevant en noodzakelijk is.

---

7 Anco Hundepool, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Eric Schulte Nordholt, Keith Spicer, Peter-Paul de Wolf, Statistical Disclosure Control, Wiley, 2012.

8 Dwork, Cynthia. 2006. Differential Privacy, 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006), Springer Verlag, 4052, 1–12, ISBN 3-540-35907-9.

9 Zie: Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille Hildebrandt, and Joeri de Ruiter: "Polymorphic Encryption and Pseudonymisation for Personalised Healthcare", IACR eprint archive paper 2016/411, https://eprint.iacr.org/2016/411).

Deze benadering helpt ook om strikte bewaartermijnen af te dwingen, en om te de verder doorgifte van persoonsgegevens strikt te controleren: er worden immers geen kopieën van de data gemaakt, dus de controle op bewaartermijnen en het beperken van de toegang tot de data door derden kan door de oorspronkelijke databeheerder worden afgedwongen.

2.2.3.5. Data labeling

Met behulp van data labeling kan context / informatie worden toegevoegd aan een bepaald gegeven. Zo kunnen gegevens bijvoorbeeld worden gelabeld als gewone, bijzondere, of strafrechtelijke gegevens. Ook kan de bron van de gegevens worden vastgelegd, het verzameldoel en de juridische basis (grondslag) voor de verwerking. Deze aanvullende informatie stelt de verwerkingsverantwoordelijke(n) vervolgens in staat om een koppeling tussen het gegeven en het gewenste gebruik ervan te maken. Deze regels kunnen zelfs worden afgedwongen in de systemen van andere organisaties (zie sticky policies hieronder).

2.2.3.6. Sticky policies (verberg / dwing af)

Ook kan er gebruik worden gemaakt van *sticky policies*. Nadat bepaald is dat een ketenpartij informatie over een persoon heeft, wordt naast de kopie van de relevante data ook een zogenaamde 'sticky policy' meegestuurd (die onlosmakelijk met de data verbonden is), welke beschrijft wat er met de die data gedaan mag worden. Idee is dat bij een interne data audit voor ieder datarecord in alle databestanden bij alle ketenpartijen zo'n sticky policy kan worden overlegd, waaruit blijkt dat dit record rechtmatig door de ketenpartner wordt verwerkt. In zo'n sticky policy kan bijvoorbeeld beschreven staan wat het doel van de verwerking van het bijbehorende datarecord is, wat de bewaartermijnen zijn, en of het record met anderen gedeeld mag worden.

Ook helpen sticky policies om strikte bewaartermijnen af te dwingen, en om te de verder doorgifte van persoonsgegevens strikt te controleren: de informatie over de bewaartermijnen en de toegangspermissies tot de data zijn permanent en onlosmakelijk aan de data gekoppeld. Een organisatie die zich niet aan de bewaartermijnen of de toegangsbeperkingen houdt kan hiervoor op de vingers worden getikt. Dit hangt dus wel af van voldoende strikte handhaving van de sticky policies.

2.3. Handhaven softdrugsbeleid

2.3.1. De casus

De wetgeving voor het gebruik van softdrugs in Nederland wordt gekenmerkt door het zogeheten gedoogbeleid. Het gedoogbeleid houdt in dat alle handelingen met het oog op softdrugs strafbaar zijn, behalve het gebruik ervan. Het in bezit hebben van softdrugs is dus ook strafbaar, maar onder bepaalde voorwaarden (zoals kleine hoeveelheden in bezit hebben) wordt het niet strafrechtelijk vervolgd. Voor het gebruik van softdrugs geldt een minimumleeftijd van 18 jaar. Coffeeshops in Nederland moeten zich voor de verkoop van softdrugs ook aan bepaalde gedoogcriteria houden, zoals het controleren van de identiteit van kopers. Bovendien worden steeds meer medewerkers van coffeeshops getraind om problematisch softdrugsgebruik te herkennen. Alhoewel er in Nederland dus strenge voorwaarden gelden voor softdrugsgebruik, blijft drugsverslaving ook onder softdruggebruikers een probleem.

Om die reden kan het in sommige gevallen nuttig zijn om persoonsgegevens van verslaafde softdrugsgebruikers uit te wisselen met andere coffeeshops. Een alternatief idee is het bouwen van een register, waarin, net als bij kansspelen, coffeeshops problematische softdrugsgebruikers kunnen registreren. Ook zouden problematische softdrugsgebruikers zichzelf in dit register kunnen inscrhijven. Op deze manier kunnen problematische softdrugsgebruikers uitgesloten worden van het kopen van drugs. Dit is echter privacygevoelig. De vraag is hoe (verslaafde) softdrugsgebruikers zelf meer controle kunnen krijgen op hun gedrag en hoe informatie over (verslaafde) softdrugsgebruikers gedeeld kan worden tussen aanbieders. Daarnaast is de vraag hoe coffeeshops de leeftijd en identiteit van softdrugsgebruikers op een veilige(re) manier kunnen verifiëren.

2.3.2. Privacyrisico's en ontwerpuitdagingen

Op basis van deze casus kunnen we de volgende privacyrisico's identificeren en daaruit de bijbehorende ontwerpuitdagingen afleiden.

2.3.2.1. Verificatie

2.3.2.1.1. *Privacyrisico's*

Coffeeshops zijn op basis van de Aanwijzing Opiumwet verplicht om vast te stellen dat de mensen die zij toegang verlenen meerderjarig zijn, maar ook dat zij ingezetenen van Nederland zijn. Het feit dat persoonsgegevens voor een coffeeshop of derde partij (zoals een leverancier van identificatiesoftware) beschikbaar zijn vormt een privacyrisico. Daarbij komt dat de gegevens door derde partijen ook mogelijk ingezet kunnen worden voor andere doeleinden.

2.3.2.1.2. *Ontwerpuitdaging*

Hoe kunnen we verifiëren dat bezoekers van coffeeshops ouder dan 18 jaar zijn en ingezetene van Nederland, zonder dat er meer persoonsgegevens worden verwerkt dan noodzakelijk en zonder dat deze persoonsgegevens verder worden verwerkt voor andere doeleinden?

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.3.3.1.

2.3.2.2. Delen van informatie tussen aanbieders

2.3.2.2.1. *Privacyrisico*

Om te voorkomen dat verslaafde softdrugsgebruikers van de ene coffeeshop naar de andere overstappen moet voor elke coffeeshop bekend zijn wat de 'status' van een softdrugsgebruiker is. Een gangbare oplossing is het bijhouden van een 'zwarte lijst'. Door middel van een centraal register kunnen problematische gebruikers dan geïdentificeerd worden. Wanneer duidelijk is dat een gebruiker bij een andere coffeeshop al bekend staat als een problematische gebruiker, dan kan de gebruiker toegang bij een andere coffeeshop (tijdelijk) worden ontzegd. Aan een dergelijke oplossing kleven echter serieuze privacybezwaren. Niet alleen kan deze lijst stigmatiserend werken als deze uitlekt, de overheid krijgt ook meer zicht op de burger.

2.3.2.2.2. *Ontwerpuitdaging*

Hoe kan je problematische softdrugsgebruikers op een veilige en privacyvriendelijke manier registreren zonder ze direct te identificeren en bepalen of een gebruiker tot een risicogroep behoort?

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.3.3.2, 2.3.3.3 en 2.3.3.4.

2.3.3. Oplossingen in het ontwerp

Aan de hand van de ontwerpstrategieën kan voor deze casus aan de volgende ontwerpkeuzes worden gedacht.

2.3.3.1. Verificatie (scheid)

Om vast te stellen of hun klanten ouder dan 18 en Nederlands staatsburger zijn kan de coffeeshop houder gebruik maken van klassieke identiteitsdocumenten als het paspoort of identiteitskaart. Hiermee krijgt de coffeeshophouder echter meer te zien dan noodzakelijk (waaronder de naam van de persoon).

Door gebruik te maken van self-sovereign identity / attribuut gebaseerde credential toepassingen wordt voorkomen dat teveel informatie wordt gedeeld. Deze toepassingen geven de ontvanger alleen toegang tot die attributen (ouder dan 18 jaar, Nederlands ingezetene) die noodzakelijk zijn om te controleren.

Voorbeelden van dergelijke toepassingen zijn Yivi en de Europese eID wallet. Zo is het bijvoorbeeld mogelijk om met behulp van Yivi door te geven of je ouder of jonger bent dan 18 jaar. In plaats van een geboortedatum door te sturen geeft Yivi aan dat de persoon ouder of jonger dan 18 is. De ontvanger kan op dit gegeven vertrouwen, omdat Yivi het antwoord ontleent aan de Basisregistratie Personen. Datzelfde geldt voor nationaliteit.

2.3.3.2. Pseudonieme en anonieme zwarte lijsten (verberg)

Om problematisch softdrugsgebruik te herkennen, kan met een zwarte lijst worden gewerkt. In plaats van het delen van zwarte lijsten met persoonsgegevens, of de coffeeshops toegang te geven tot een centrale database met deze gegevens, kan een zwarte lijst ook op basis van pseudoniemen worden bijgehouden. Dit begint met het uitgeven van een pseudonieme identiteit door een trusted third party (TTP). Gebruikers moeten zich identificeren bij deze TTP en deze TTP geeft vervolgens een pseudonieme identiteit uit. Wanneer er aanleiding is om een gebruiker te weren, dan kan dit worden teruggekoppeld aan de TTP, die ervoor zorgt dat deze informatie wordt gedeeld met andere coffeeshops. Ook zou de aanbieder zelf deze gepseudonimiseerde gegevens kunnen doorgeven aan de andere coffeeshops.

Deze oplossing kan ook gebruikt worden in combinatie met de eerder genoemde decentrale verificatie oplossingen. In dit scenario moet de gebruikers niet alleen verifiëren dat zij 18+ en Nederlands ingezetene zijn, maar ook dat ze beschikken over een ‘geldig toegangsbewijs’. Het bewijs dat de gebruiker toegang mag krijgen kan in de vorm van een token worden uitgegeven door de TTP.

Deze oplossing voorkomt dat de coffeeshophouders onderling te weten komen wie een problematische gebruiker is. Ook voorkomt het het lokaal moeten bijhouden van zwarte lijsten en het delen van deze lijsten. Wel is een centrale autoriteit (de TTP) noodzakelijk. De reden hiervoor is dat je een ‘echte’ nieuwe bezoeker moet kunnen onderscheiden van een terugkerende bezoeker die gewoon een nieuw profiel heeft aangemaakt (omdat het oude profiel bijvoorbeeld een registratie als probleemgebruiker bevatte). De TTP kan ervoor zorgen dat iemand zich niet opnieuw kan registreren.

2.3.3.3. Blacklistable anonymous credentials (scheid / verberg)

In de bovenstaande oplossing weet de TTP nog steeds op welke persoon de gegevens betrekking hebben. Dit is een kwetsbaarheid. Een oplossing die de privacy nog verder beschermt, is om voor toegang tot de coffeeshop gebruik te maken van zogenaamde *blacklistable anonymous credentials*. Dit is ook een vorm van self-sovereign identity / attribuut gebaseerde credential (zie boven) waarbij de credential naderhand geblokkeerd/herroepen kan worden.[10] Echter, in deze opzet wordt niet langer gebruik gemaakt van een TTP voor het bijhouden van de zwarte lijst. De aanbieder (de coffeeshophouder) kan in plaats daarvan zelf de gebruiker blokkeren op basis van diens gedrag en dit gegeven delen via een publiek register (een

10 Zie: https://www.cs.dartmouth.edu/~sws/pubs/aktso7.pdf.

append-only public ledger).[11] Zowel het authenticeren tegen dit register als het onderhoud ervan kan anoniem plaatsvinden waardoor de privacy van de bezoeker gewaarborgd is. [12]

2.3.3.4. Decentraal registreren gebruik (scheid)

Wanneer het noodzakelijk is om het softdrugsgebruik van de gebruiker te monitoren (bijvoorbeeld om vast te stellen of er sprake is van problematisch gebruik), is de meest privacyvriendelijke manier om dit decentraal te doen. Het softdrugsgebruik wordt niet bij de coffeeshops opgeslagen, maar in een 'digitale kluis' (personal data store) van de gebruiker zelf. Coffeeshops krijgen het recht om daar informatie aan toe te voegen (anders mag de gebruiker geen drugs kopen), maar kunnen niet zondermeer detailinformatie uit de kluis teruglezen. Wat coffeeshops wel kunnen doen is de digitale kluis van een gebruiker vragen of deze problematisch drugsgebruik vertoont, door de vraag (als een functie van geregistreerde waarden in de kluis) op te sturen, en het (gevalideerde) antwoord van de kluis terug te ontvangen, op basis van deze onderliggende waarden. Een alternatief is dat de gebruikers zelf hun drugsgebruik kunnen bewaken op basis van de gegevens in hun digitale kluis, en de kluis eventueel zelf automatisch waarschuwingen kan laten genereren als grenswaarden worden overschreden.

Het voordeel van het gebruik van personal data stores is dat ook gebruikers die gelijktijdig bij verschillende coffeeshops drugs kopen, en die bij elk van die bedrijven individueel onder de radar zouden blijven, alsnog gewaarschuwd of geweerd kunnen worden als hun cumulatieve drugsgebruik daartoe aanleiding geeft.

Voorbeeld van personal data stores zijn Qiy en Solid.

2.4. Preventie gokverslaving

2.4.1. De casus

Sinds 2021 is het mogelijk om legaal online te gokken. Aanbieders van online kansspelen die een vergunning hebben mogen deze spelen nu aanbieden aan consumenten. Hoewel online gokken leuk en spannend kan zijn, levert het voor sommige spelers helaas ook grote risico's op, zoals problematische gokschulden en verslaving. Om de risico's van het online gokken te verkleinen moet er een zekere mate van controle zijn op spelers. De aanbieders van online kansspelen hebben hier een wettelijke verantwoordelijkheid. Zij moeten om te beginnen registreren hoe vaak een speler komt spelen. Ook moeten zij spelers observeren en monitoren. Als speelgedrag daartoe aanleiding dan moet de aanbieder in gesprek gaan met de speler. De aanbieder moet alle interventies registreren en daar een dossier van bijhouden.

Echter, uit onderzoek van toezichthouder de Kansspelautoriteit blijkt dat veel online gokbedrijven te weinig doen om spelers te beschermen tegen gokverslaving. Zo stelt de bestuursvoorzitter van de Kansspelautoriteit dat aanbieders de grenzen van hun zorgplicht mogelijk ver overschrijden.[13] Zonder tijdige signalering van gokbedrijven kunnen er dus al veel problemen ontstaan. Dit is met name het geval wanneer spelers over meerdere sites heen gokken. Dit is echter privacygevoelig. De vraag is hoe (problematische) spelers zelf meer controle kunnen krijgen op hun gedrag en hoe gegevens over problematische spelers gedeeld kunnen worden tussen aanbieders.

11 Pseudonieme en volledige anonieme credential systemen werken het best in een online omgeving waar de aanbieder de gebruiker niet kan zien. In de fysieke wereld is het natuurlijk mogelijk dat de aanbieder (de coffesehophouder) de persoon herkent op basis van diens fysieke kenmerken.

12 Zie: Yang, R. et al. (2019), Decentralized blacklistable anonymous credentials with reputation, in: Computers & Security, Volume 85, 2019, pp. 353-371.

13 https://nos.nl/artikel/2490171-online-gokbedrijven-verzaken-zorgplicht-spelers-verliezen-veel-in-korte-tijd.

2.4.2. Privacyrisico's en ontwerpuitdagingen

Op basis van deze casus kunnen we het volgende privacyrisico identificeren en daaruit de bijbehorende ontwerpuitdaging afleiden.

2.4.2.1. Monitoren gokgedrag

2.4.2.1.1. *Privacyrisico*

In hun spelersaccount geven spelers onder meer aan hoeveel geld zij willen en kunnen verspelen, hoe lang zij willen spelen en hoe vaak. Als het speelgedrag daarvan afwijkt, is de aanbieder verplicht de speler daarvan op de hoogte te stellen. Het feit dat deze informatie geregistreerd staat vormt een risico voor de privacy omdat deze informatie kan lekken, maar ook omdat de aanbieder de gegevens voor andere doelen dan monitoring kan gebruiken. De hoeveelheid geld bijvoorbeeld die iemand kan 'missen' zegt iets over de financiële draagkracht van deze persoon. Een aanbieder zou deze informatie kunnen misbruiken.

2.4.2.1.2. *Ontwerpuitdaging*

Hoe kunnen we spelers waarschuwen voor afwijkingen in de parameters die ze zelf stellen voor hun gokgedrag, zonder dat we deze gegevens permanent delen met de aanbieder?

Oplossingen voor dit risico en de ontwerpuitdaging kunnen gevonden worden in 2.4.3.1 en 2.4.3.2.

2.4.3. Oplossingen in het ontwerp

2.4.3.1. Lokale monitoring (scheid)

Monitoring kan in de (web)app van de gokaanbieder op het apparaat van de gebruiker zelf geïmplementeerd worden. De gebruiker legt zijn voorkeuren (inzetlimieten, maximale verliezen per dag, maximale speeltijd per dag/week) lokaal vast in de app, en de app monitort continue of deze grenzen worden overschreden. Dit is vergelijkbaar met hoe nu ook al app gebruikslimieten op sommige smartphones kunnen worden ingesteld.

2.4.3.2. Informatie (informeer/geef controle)

Om gebruikers bewust te maken van het feit dat hun gokgedrag actief gemonitord en geregistreerd wordt kunnen waarschuwingen gebruikt worden. Naast dat dit bijdraagt aan het transparantiebeginsel, kan dit ook helpen om spelers op een continue manier te wijzen op hun gokgedrag. Waarschuwingen kunnen door middel van (mini)dashboards getoond worden aan gebruikers bij het spelen. Zo kunnen verschillende staafdiagrammen getoond worden waarvan elk een ander onderwerp weergeeft. Een diagram geeft bijvoorbeeld actief het bedrag dat iemand heeft weggespeeld weer, een andere de hoeveel tijd die gespeeld is en een derde kan bijvoorbeeld gebruikt worden om de limieten van een gebruiker aan te geven.

3. Overzicht Ontwerppatronen en PETS

In dit hoofdstuk geven wij een overzicht van PETs die gebruikt kunnen worden om producten, processen, diensten en toepassingen privacy vriendelijker te maken.

3.1. Domein- of dienst-specifieke pseudoniemen

Uitleg	Strategieën	Toepassingen en bronnen
Pseudoniemen zijn een goede manier om data niet direct herleidbaar te maken tot een persoon. Vaak worden pseudoniemen echter automatisch uit de naam of het BSN van de persoon berekend. Als iedere dienst dezelfde methode hiervoor gebruikt, dan zou dezelfde persoon bij al deze diensten hetzelfde pseudoniem hebben, en zouden zijn of haar data bij elk van deze diensten alsnog koppelbaar zijn. Om dat te voorkomen kunnen dienst specifieke pseudoniemen gebruikt worden. In essentie betekent dat dat elke dienst zijn eigen, volledige andere, methode voor het automatisch bepalen van pseudoniemen gebruikt. Om dit in de praktijk ook makkelijk en controleerbaar te maken, is een bekende methode om de naam of code van de dienst zelf mee te nemen in een gestandaardiseerde methode voor het bepalen van een pseudoniem. Vaak wordt hier een hashfunctie voor gebruikt. Het pseudoniem voor persoon X bij dienst A is dan Pseudoniem(X,A)=Hash(X,A) en voor dienst B is dat Pseudoniem(X,B)=Hash(X,B). De eigenschappen van de hashfunctie zorgen ervoor dat de twee pseudoniemen niet aan elkaar gerelateerd kunnen worden, en ook dat de identiteit van X zelf er niet uit gereconstrueerd kan worden.	Verberg	

3.2. Personal data stores

Uitleg	Strategieën	Toepassingen en bronnen
Personal data stores (PDS) geven mensen nieuwe mogelijkheden om hun gegevens zelf te beheren. In plaats dat bij iedere organisatie of instantie een kopie van allerlei (persoons)gegevens bijgehouden wordt, beheert en bewaart de gebruiker deze gegevens zelf in zijn eigen 'digitale kluis'. De bedrijven en instellingen krijgen vervolgens enkel toegang tot de voor hun relevante gegevens in deze kluis. Voordeel is dat de gebruiker een gegeven slechts eenmaal hoeft te wijzigen, waarna alle afhankelijke partijen in één keer van de wijziging op de hoogte zijn. Ook kan de gebruiker op een willekeurig moment beslissen om de toegang tot bepaalde gegevens voor een bedrijf of instelling te beperken. Met andere woorden: de gebruiker krijgt zelf veel meer controle over zijn (persoonlijke) data.	Controleer, Scheid, Verberg	QIY, PiM, Solid

3.3. Self sovereign identity / attribuut gebaseerde credentials

Uitleg	Strategieën	Toepassingen en bronnen
Centraal bij self-sovereign identity / attribuut gebaseerde credentials staat het concept van een credential: een gewaarmerkte uitspraak over een persoonlijke eigenschap, bijvoorbeeld iemands leeftijd of opleidingsniveau. Deze credentials kunnen door willekeurige partijen uitgegeven worden (zelfs door individuele gebruikers). Een credential wordt éénmaal (voor een bepaalde geldigheidsduur) uitgegeven, en kan vervolgens meerdere malen door de houder gebruikt worden om aan tonen dat hij of zij de betreffende persoonlijke eigenschap heeft. Credentials worden opgeslagen in wallets; dit kan op de smartphone van de gebruiker zijn, of ergens in de cloud. De wallet wordt gebruikt om te beslissen óf en zo ja welke credentials aan een controlerende dienstaanbieder getoond worden. Deze 'selective disclosure' zorgt ervoor dat de gebruiker zelf de controle heeft over het delen van zijn of haar persoonlijke eigenschappen. Wanneer de gebruiker een bepaalde dienst wil gebruiken, vraagt de dienst aan de gebruiker een bepaald bewijs, bijvoorbeeld dat hij een man/vrouw is. De gebruiker kiest er vervolgens voor om dit vrij te geven aan de dienst via zijn telefoon. Het is aan de controlerende partij om te beslissen welke credentials geaccepteerd worden. Zo kan een dienstaanbieder er voor kiezen om een 'man/vrouw-credential' over de zelfde persoon uitgegeven door drie verschillende mensen gelijk te stellen aan een 'man/vrouw-credential' uitgegeven door de Nederlandse overheid.[14] Self-sovereign identity (SSI) heeft raakvlakken met personal data stores (PDS).	Controleer, Scheid, Verberg	Yivi, eIDAS V2 identity wallet

14 https://www.surf.nl/en/what-is-self-sovereign-identity.

3.4. Dashboards

Uitleg	Strategieën	Toepassingen en bronnen
Een organisatie die persoonsgegevens van gebruikers verwerkt, kan tegelijkertijd gebruikers toegang verlenen tot hun eigen gegevens door middel van een dashboard of 'mijn' omgeving. Om transparantie te garanderen, moet het systeem op efficiënte wijze het type en de reikwijdte tonen van de verschillende persoonsgegevens die door de organisatie (als verwerkingsverantwoordelijke) worden verwerkt. Het doel van de implementatie van een dergelijk dashboard is om gebruikers (betrokkenen) voldoende informatie te geven over de verwerking van hun persoonsgegevens en ze in staat te stellen dit beter te begrijpen. Daarnaast kan het gebruik van transparante dashboards ervoor zorgen dat de verwerkingsverantwoordelijke voorzichtiger is in het maken van keuzes rondom bijvoorbeeld het delen van persoonsgegevens. In het dashboard zijn samenvattingen van persoons-gegevens op een begrijpelijke manier weergegeven. Deze weergave kan verschillende vormen aannemen, waaronder illustraties, voorspellende modellen, visuele representaties of statistische gegevens. Bij het opstellen van een dashboard kan rekening worden gehouden met de 5 verschillende elementen uit het framework 'privacy mirrors.'[15] Ook loggen kan een middel zijn om deze doelen te bereiken. De 5 elementen van privacy mirrors zijn: 1. Het bijhouden van de historie van gegevensstromen; 2. Gebruikers in staat te stellen om feedback te geven en keuzes te maken in wat zij willen weten over hun gegevens; 3. Het bevorderen van bewustzijn bij gebruikers op verschillende vlakken, zoals sociaal, technisch en fysiek; 4. Het afleggen van verantwoording over wie toegang heeft en wie wat doet met gegevens; 5. Gebruikers in staat stellen om veranderingen door te voeren (mede op basis van de vorige stappen). 6. Naast het informeren van betrokkenen kunnen dashboards ook gebruikt worden om persoonsgegevens aan te passen.	Controleer, Scheid, Verberg	Yivi, eIDAS V2 identity wallet

15 https://www.privacypatterns.org/patterns/Privacy-Mirrors.html.

3.5. Zero Knowledge-proofs

Uitleg	Strategieën	Toepassingen en bronnen
Zero-knowledge proofs[16] zijn cryptografische hulpmiddelen die effectief de beginselen van vertrouwelijkheid en dataminimalisatie kunnen handhaven. Een zero-knowledge proof stelt een betrokkene in staat om aan een verwerkingsverantwoordelijke aan te tonen dat hij of zij over bepaalde vertrouwelijke informatie beschikt zonder specifieke informatie over die vertrouwelijke gegevens vrij te geven. Dit gaat in sommige gevallen zelfs zo ver, dat de partij die de zero knowledge proof controleert zelfs een willekeurige andere partij er niet van kan overtuigen dat het bewijs klopt (en dat de betrokkene op de hoogte is van de vertrouwelijke informatie). Zelf weet de controlerende partij dat echter wel zeker. Zero-knowledge proofs zorgen er niet alleen voor dat de vertrouwelijkheid wordt behouden, maar ook dat de data geminimaliseerd wordt. Dit in tegenstelling tot andere authenticatiemethoden, zoals het invullen van een gebruikersnaam en wachtwoord. Bij deze authenticatiemethode wordt het wachtwoord vergeleken met het wachtwoord dat is opgeslagen op de server van de verwerkingsverantwoordelijke. Een hacker kan dan proberen om of het wachtwoord van de server te stelen of het wachtwoord van de gebruiker te stelen. Echter, door gebruik te maken van Zero-knowledge proofs ligt dit risico alleen nog bij de gebruiker, omdat de server niet weet welke geheime informatie gebruikt wordt voor de authenticatie. Een zero-knowledge proof kan ook gebruikt worden om te bewijzen dat men een bepaald credential met een persoonlijke eigenschap bezit (bijvoorbeeld dat men ouder is dan 18 jaar), zonder het daadwerkelijke credential te tonen. Dit zorgt ervoor dat het gebruik van dit specifieke credential (vaak met unieke serienummers of digitale handtekenignen van de uitgevende instantie) niet gevolgd of gekoppeld kan worden aan eerder gebruik van dat credential. Het maakt het gebruik van credentials en is dus onlinkbaar en daarmee zo anoniem mogelijk. Deze methode beperkt de hoeveelheid gegevens die de server over de gebruiker heeft aanzienlijk, waardoor het potentiële aanvalsoppervlak kleiner wordt. Met betrekking tot Zero-knowledge proofs zijn er twee varianten: interactief en niet-interactief. Interactieve Zero-Knowledge proofs vereisen meerdere uitwisselingen tussen gebruiker en de server voor authenticatie. Daarentegen vereisen niet-interactieve Zero-Knowledge Proofs geen enkele communicatie. Deze niet-interactieve variant is bijvoorbeeld erg populair bij blockchain applicaties. Zero-knowledge proofs liggen ook aan de basis van veel secure multiparty computation protocollen, en aan onlinkbaar gebruik van attribuut gebaseerde credentials (zie boven).	Minimaliseer, Verberg	Starkware, ING's Zero-Knowledge Range Proof solution, Zcash (ZK-Snarks),

16 European Union Agency of Cybersecurity & ENISA, "Data Protection Engineering: From Theory to Practice", January 2022, p.22

3.6. Private Information Retrieval

Uitleg	Strategieën	Toepassingen en bronnen
Private information retrieval (PIR)[17] is een cryptografische methode die is ontworpen om gebruikers toegang te geven tot specifieke items in een database zonder aan de gegevensbeheerder, zoals de eigenaar of beheerder van de database, bekend te maken welk specifiek item wordt opgevraagd. Het doel van het implementeren van PIR is om de onthulling van informatie over het opgevraagde element te minimaliseren, zodat de gegevensbeheerder niet weet welke items zijn opgevraagd. In essentie dient PIR als een privacybeschermend mechanisme waarmee gebruikers discreet informatie uit een database kunnen opvragen. PIR maakt het bijvoorbeeld mogelijk om een record over een bepaald persoon in een database op te vragen, zonder dat de database beheerder kan zien over wie informatie is opgevraagd. Deze zeer sterke mate van privacybescherming heeft wel consequenties qua performance: de codering van de vraag is vaak omvangrijk (het moet immers verbergen wat er precies gevraagd wordt), en datzelfde geldt voor (het berekenen van) het antwoord.	Minimaliseer	

17 European Union Agency of Cybersecurity & ENISA, “Data Protection Engineering: From Theory to Practice”, January 2022, p.16-17.

3.7. Polymorfe encryptie (PEP)

Uitleg	Strategieën	Toepassingen en bronnen
Het nadeel van standaard encryptiemethoden is dat op het moment van versleutelen bekend moet zijn wie de toekomstige ontvanger of lezer van de data is: dit bepaalt immers welke sleutel gebruikt moet worden. Dit is echter niet altijd op voorhand bekend. In deze gevallen biedt polymorfe encryptie uitkomst[18]. Polymorfe encryptie werkt als volgt: Gebruikers moeten zich aanmelden voor de dienst en krijgen een sleutel voor polymorfe encryptie toegewezen. Daarmee kunnen ze data versleutelen, en deze data zelf ook later weer ontsleutelen. Versleutelde data kan op deze wijze veilig opgeslagen worden, bijvoorbeeld in een cloud omgeving. Op een willekeurig later moment kan bepaald worden wie de data mag ontsleutelen. Deze beslissing wordt genomen op basis van een beleid, waarin de betrokkene een centrale rol moet spelen. Hij of zij kan besluiten dat persoon X,Y,Z hun data mogen ontsleutelen om ze te gebruiken voor specifieke doeleinden. Het zogeheten 'tweaken' van de versleutelde data om ze ontsleutelbaar te maken voor een specifieke partij kan op een 'blinde' manier gebeuren door een zogenaamde Transcriptor. Deze Transcriptor krijgt de oorspronkelijke onversleutelde data dus niet te zien. Op deze manier kunnen mensen hun gegevens met behulp van polymorfe versleuteleling veilig opslaan. Daarnaast kunnen ze later beslissen (om delen van) hun data beschikbaar te maken (te ontsleutelen) voor specifieke partijen, voor specifieke analyse doeleinden. Zo houden gebruikers de controle en kunnen ze controleren welke gegevens waar worden gebruikt en voor welke doeleinden.	Verberg	Starkware, ING's Zero-Knowledge Range Proof solution, Zcash (ZK-Snarks),

18 https://eprint.iacr.org/2016/411.pdf.

3.8. Polymorfe pseudoniemen (PEP)

Uitleg	Strategieën	Toepassingen en bronnen
Polymorfe pseudoniemen[19] zijn een variant van polymorfe encryptie, die het mogelijk maakt om (weer met behulp van een 'blinde' Transcriptor) iemands pseudoniem voor de ene dienst om te zetten naar zijn of haar pseudoniem voor een andere dienst. Polymorfe pseudoniemen lijken dus op dienst specifieke pseudoniemen (zie boven) die echter in elkaar kunnen worden omgezet (door de Transcriptor) als daarvoor door de betrokkene, of op basis van beleidsregels, toestemming voor is gegeven.	Verberg	

19 Eric Verheul et al., ''Polymorphic Encryption and Pseudonymisation for Personalised Healthcare,'' 30 september 2016, p. 6.

3.9. Afdwingen privacy policies en privacyverklaringen

Uitleg	Strategieën	Toepassingen en bronnen
Door de implementatie van de juiste privacy policies zorgen organisaties ervoor dat er transparant met de verwerking van persoonsgegevens wordt omgegaan. Het bereiken van een balans tussen een gebruiksvriendelijke weergave van privacyregels en de vereiste juridische achtergrond vormt daarbij een uitdaging.[20] Het kan namelijk ingewikkeld zijn voor gebruikers om privacyregels te begrijpen, vooral in complexe situaties. Over het algemeen is gebleken dat gebruikers juist liever relevante en beknopte informatie ontvangen dan een grote hoeveelheid informatie in één keer. Bij het opstellen van privacygerelateerde informatie is het daarom van belang om makkelijke en gebruikelijke taal te gebruiken en dat ook wordt nagedacht dat niet iedereen bekend is met de relevante gegevensbescherming en privacy-terminologie. Voorbeelden van duidelijke privacyverklaringen en beleidstukken zijn de: • 3-gelaagde verklaring (3-tiered notice). Dit is een privacyverklaring die bestaat uit korte kennisgeving (met kerninformatie), verkorte kennisgeving (met rechten van de betrokkene, rechtsgrondslag, enz) en de volledige kennisgeving. Deze structuur moet voorkomen dat de gebruiker 'informatiemoe' wordt.[21] • Tooltips: Om geïnformeerde toestemming van gebruikers te verkrijgen, zelfs als ze het beleid misschien niet lezen en gewoon de dienst willen gaan gebruiken, kunnen beheerders gebruikers op een onopvallende manier van informatie voorzien door middel van 'tooltips' (via de muisaanwijzer). Dit betekent dat op het moment dat een gebruiker over een object of tekst heen beweegt met zijn muis, er extra informatie of toelichting verschijnt in bijvoorbeeld een tekstwolkje. Pas, waar mogelijk, de applicatie-instellingen aan zodat ze overeenkomen met de voorkeuren die het meest overeenkomen met deze gebruikerskeuzes. Het is belangrijk om te erkennen dat gebruikers niet noodzakelijkerwijs de voorkeur geven aan de standaardinstellingen die door de organisaties zijn ingesteld, zelfs als deze standaardinstellingen zijn ontworpen met privacyoverwegingen in het achterhoofd.	Dwing af, Informeer	Tosdr.org

20 https://privacypatterns.org/patterns/Privacy-Policy-Display.html

21 Article 29 data protection working party, Guidelines on transparency under regulation 2016/679, 19.

3.10. Het gebruik van iconen

Uitleg	Strategieën	Toepassingen en bronnen
In aanvulling op een privacy policy of verklaring, kunnen Privacyiconen of pictogrammen ingezet worden om onder andere categorieën gegevens, middelen, doeleinden en legitieme belangen aan te geven. Ook in de AVG wordt het gebruik van dergelijke iconen benoemd.[22] Een goede manier om deze iconen in te zetten is om ervoor te zorgen dat de iconen gestandaardiseerd, duidelijk, consistent maar ook onderscheidbaar zijn. Van belang is dat de pictogrammen op gepaste wijze gegroepeerd worden en het moet mogelijk zijn om verdere informatie te verstrekken aan geïnteresseerde gebruikers. Belangrijk daarbij is dat de pictogrammen niet een op zichzelf staand middel zijn om privacyinformatie te verschaffen, maar een aanvulling vormen. In artikel 12 van de AVG wordt de nadruk dan ook gelegd op 'in combinatie met.' In een richtsnoer van de European Data Protection Board wordt het belang van het gebruik van iconen in het kader van verbeterde transparantie tevens benadrukt.[23] Een aangeraden methode voor de implementatie van iconen is het implementeren van een systeem dat gestandaardiseerde kleuren gebruikt om gebruikers te helpen privacyvriendelijke keuzes te maken en het bijbehorende beleid te begrijpen. Zo kunnen verschillende privacyinstellingen onderverdeeld worden in verschillende niveaus, elk weergegeven door een specifieke kleur. Gebruikers zien deze kleuren dan als indicatoren van hun huidige privacyinstellingen tijdens relevante acties. Een voorbeeld van een dergelijke gestandaardiseerde kleur kan bijvoorbeeld rood zijn voor waarschuwingen.[24]	Dwing af, Informeer	Tosdr.org

22 AVG art. 12, lid 7.

23 Article 29 data protection working party, Guidelines on transparency under regulation 2016/679, 25-26.

24 https://privacypatterns.org/patterns/Privacy-color-coding.

3.11. Secure Multi-party Computation

Uitleg	Strategieën	Toepassingen en bronnen
Secure Multi-Party Computation[25] (MPC) is een vorm van PET die meerdere partijen in staat stelt om gezamenlijk een functie over hun invoer te berekenen, terwijl hun invoer privé blijft. Met andere woorden, Secure Multi-Party Computation zorgt ervoor dat een groep partijen geaggregeerde gegevens kan berekenen door overeen te komen hoe de verwerking zal plaatsvinden. Tegelijkertijd kan geen van de partijen iets te weten komen over de ruwe data die door de andere partijen als invoer worden geleverd. De deelnemende partijen werken voor het berekenen van de uitkomst samen op basis van een vooraf afgesproken protocol, waarin wordt vastgelegd welke informatie, met wie, op welk moment en met welke vorm van versleuteling moet worden gedeeld of in een berekening moet worden verwerkt, Naarmate het aantal deelnemers toeneemt moeten er onderling tussen meer partijen gegevens worden uitgewisseld: de communicatiebelasting neemt dus significant toe, daarmee is Secure Multiparty Computation dus vaak ook tijdrovender vanwege de latentie die inherent is aan het onderling moeten communiceren van grote hoeveelheden versleutelde gegevens.	Minimaliseer, Scheid	TNO

3.12. Private set intersection protocol

Uitleg	Strategieën	Toepassingen en bronnen
Een specifiek casus van veilige MPC is het private set intersection protocol, waarin twee partijen met private lijsten met waarden de intersectie van de lijsten willen vinden, zonder iets anders te onthullen dan de elementen in de intersectie. Er bestaan hier verschillende MPC-protocollen voor.	Verberg	NIST

25 European Union Agency of Cybersecurity & ENISA, “Data Protection Engineering: From Theory to Practice”, January 2022, p.14; 4.

3.13. Personal health train

Uitleg	Strategieën	Toepassingen en bronnen
De personal health train (PHT), is een samenwerking van TNO en verschillende organisaties die het Connect2HealthConsumer zijn gestart. Dit is een project wat gericht is op het ontwikkelen van technologieën, standaarden en afspraken om allerlei gezondheidsdata met elkaar te verbinden en tegelijkertijd de privacy van de betrokkene te beschermen. Het principe van PHT is dat de data waarop je analyses wilt uitvoeren niet vanuit verschillende databronnen op een plek centraal verzameld wordt, maar beschikbaar komen via de verschillende databronnen. De analyse wordt naar de data gebracht en gaat dan als een trein via een technische infrastructuur (de rails) naar de verschillende databronnen (de stations).[26] Stations kunnen variëren van grote kerndatabases tot kleine persoonlijke kluizen die de gegevens van één individu bevatten. Een station heeft daarnaast ook huisregels. Zo heeft elk gegevenselement een bijbehorende licentie die beschrijft wat een bezoekende trein met dat gegevenselement mag doen. Stations worden gebouwd en onderhouden door vertrouwde partijen en beheerd door de eigenaar van de gegevens. Treinen zijn 'workflows' die specifieke onderzoeksvragen of use cases uitvoeren waarvoor gegevens nodig zijn. Treinen kunnen groot zijn, maar ook klein of specifiek. Treinen worden meestal gebouwd en onderhouden door een onderzoeker. Het spoor bepaalt, onderhoudt en controleert de interactieregels en is de interface tussen treinen en stations. Alle onderzoekstreinen die gecertificeerd zijn en stations die gecertificeerd zijn, zijn toegestaan op het spoor.[27] De gebruiker kan zowel een organisatie als de betrokkene zelf zijn. De PHT kan dan een antwoord leveren op basis van verschillende gegevensbronnen, en zal zelf pas de data gebruiken na uitdrukkelijke toestemming van de eigenaar zelf.[28]	Minimaliseer, Scheid	TNO

26 https://iknl.nl/nieuws/2021/personal-health-train-kansen-voor-onderzoek-bij-ze.
27 https://www.dtls.nl/fair-data/personal-health-train/.
28 https://www.tno.nl/nl/newsroom/2020/09/consortium-start-ontwikkeling-privacy/

3.14. Blacklistable anonymous credentials

Uitleg	Strategieën	Toepassingen en bronnen
Geanonimiseerde intrekbare credentialsystemen bieden dienstverleners een manier om gebruikers te verifiëren op basis van hun historisch gedrag en garanderen tegelijkertijd dat alle gebruikers op een anonieme en niet te koppelen manier, toegang hebben tot diensten. Over het algemeen registreert een gebruiker die toegang wil tot de diensten van een dienstverlener zichzelf eerst bij de credential-verstrekker ('credential issuer') en krijgt hij een credential terug. Vervolgens vraagt de gebruiker de dienstverlener om een policy en bewijst hij aan de dienstverlener dat hij een geldige credential heeft. Daarnaast bewijst hij dat hij voldoet aan de policy van de dienstverlener iedere keer als hij toegang wil krijgen tot de diensten van de dienstverlener. Vervolgens wordt het gedrag van de gebruiker beoordeeld door de dienstverlener nadat hij klaar is met het gebruik van diensten. De credential kan worden ingetrokken als deze beoordeling negatief uitvalt.[29]	Verberg	

3.15. Notification patterns (asynchronous / ambient)

Uitleg	Strategieën	Toepassingen en bronnen
Het is belangrijk dat gebruikers zich realiseren dat hun gegevens worden verwerkt, worden geïnformeerd. Hoewel gebruikers moeten worden geïnformeerd, moet de informatie ze niet overweldigen. Het weergeven van discrete, maar goed zichtbare meldingen zonder dat dit de activiteiten van de gebruiker verstoort, kan een manier zijn om gegevensverwerkingen onder de aandacht te brengen. Daarnaast kunnen meldingen bijvoorbeeld een samenvatting bevatten van recentelijk verzamelde gegevens (vanaf de laatste kennisgeving) om gebruikers te herinneren aan de gegevensverzameling.	Informeer	

29 Yang et al., ''Decentralized blacklistable anonymous credentials with reputation,'' 2019, https://www.sciencedirect.com/science/article/abs/pii/S0167404818313282#:~:text=Blacklistable%20anonymous%20credential%20systems%20provide,are%20potentially%20useful%20in%20practice.

3.16. Anonimisering

Uitleg	Strategieën	Toepassingen en bronnen
Wanneer het niet (langer) noodzakelijk is om gegevens te koppelen aan een individu, dan moeten deze verwijderd of geanonimiseerd worden. Anonieme datasets kunnen gebruikt worden om analyses te doen en inzichten te krijgen in een bepaalde populatie. Technieken om datasets te anonimiseren zijn bijvoorbeeld perturbatie, afscherming (masking) en generalisatie. Houd er wel rekening mee dat een geanonimiseerde dataset 'gedeanonimiseerd' kan worden wanneer de anonimisering niet voldoende robuust is. Om de robuustheid van anonimisering te kunnen beoordelen kan gebruik worden gemaakt van concepten als k-anonimity. L-diversity en t-closeness. Een alternatief voor het verzamelen en anonimiseren van persoonsgegevens voor bijvoorbeeld software testen is gebruik maken van synthetische datasets.	Abstraheer	Working Party 29 Opinion on Anonymisation techniques 05/2014 Uitleg CBS synthetische data

4. Veelvoorkomende privacyrisico's, ontwerpuitdagingen en oplossingsrichtingen

In dit hoofdstuk bespreken wij enkele veelvoorkomende privacyrisico's en ontwerpuitdagingen. Op basis daarvan doen wij suggesties voor oplossingen met behulp van de PETs die genoemd zijn in het vorige hoofdstuk. Deze lijst kan bijvoorbeeld gebruikt worden tijdens het doen van DPIAs om risico's te identificeren en risicobeperkende maatregelen voor te stellen.

1. Identificatie		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Prijsgeven van te veel informatie bij identificatie en autorisatie.	Robuuste identificatie terwijl zo min mogelijk gegevens worden gedeeld met de aanbieder.	• Robuuste identificatie / authenticatie methoden (bijvoorbeeld DigiD). • Self-sovereign identity.

2. Verificatie		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Bij het verifiëren van eigenschappen van de gebruiker (bijvoorbeeld is iemand 18+) wordt te veel informatie doorgegeven (bijvoorbeeld het hele paspoort, of iemands geboortedatum).	Zorgen dat de verificatie voldoende robuust is zodat de aanbieder erop kan vertrouwen, zonder te veel gegevens prijst te geven.	• Self-sovereign identity / attribuut gebaseerde credential systemen.

3. Informatie over de verwerking van persoonsgegevens		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Betrokkenen hebben geen zicht op de verwerking van hun persoonsgegevens.	Zorgen dat personen (contextueel) geïnformeerd worden over de verwerking van hun persoonsgegevens	• Privacy dashboards. • Gebruik van iconen. • Afdwingen privacy policies en notices. • Personal data stores. • Notification patterns.

4. Controle over persoonsgegevens		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Betrokkenen hebben geen of te weinig controle op hun eigen persoonsgegevens.	Zorgen dat personen controle kunnen uitoefenen op de verwerking van hun eigen gegevens.	• Privacy dashboards. • Personal data stores.

5. Bijeenbrengen / matchen gegevens		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Partijen delen (te veel) gegevens bij het beoordelen of er sprake is van een match tussen personen in hun databases.	Bepalen of de andere organisatie iets weet van een persoon zonder prijs te geven over welke persoon het gaat aan deze organisatie.	• Secure Multi Party Computation (private set intersection protocol).

6. Herleidbaarheid personen		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Gegevens van een persoon kunnen aan deze persoon worden gekoppeld.	Het verkleinen van de kans dat gegevens betreffende een persoon door een derde kunnen worden gekoppeld aan diens werkelijke identiteit.	• (polymorfe) pseudoniemen • Anonimisering gegevens. • Domein-specifieke pseudonimisering.

7. Insluiten / uitsluiten personen		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Zwarte lijsten hebben een sterk stigmatiserend effect op personen.	Het kunnen insluiten / uitsluiten van personen zonder dat hun persoonsgegevens gedeeld worden.	• Self-sovereign identity / attribuut gebaseerde credential systemen. • Anonymous blacklistable credentials.

8. Monitoren gedrag		
Privacyrisico	**Ontwerpuitdaging**	**Oplossingsrichting**
Het monitoren van het gedrag van personen geeft een indringend beeld van een deel van het persoonlijke leven.	Het kunnen beoordelen of iemand voldoet aan bepaalde criteria / regels, zonder dat daarvoor gegevens over de betrokkene centraal worden opgeslagen.	• Decentrale opslag / personal data stores. • Privacy dashboards.

5. Bijlage: **Achtergrond Privacy by Design**

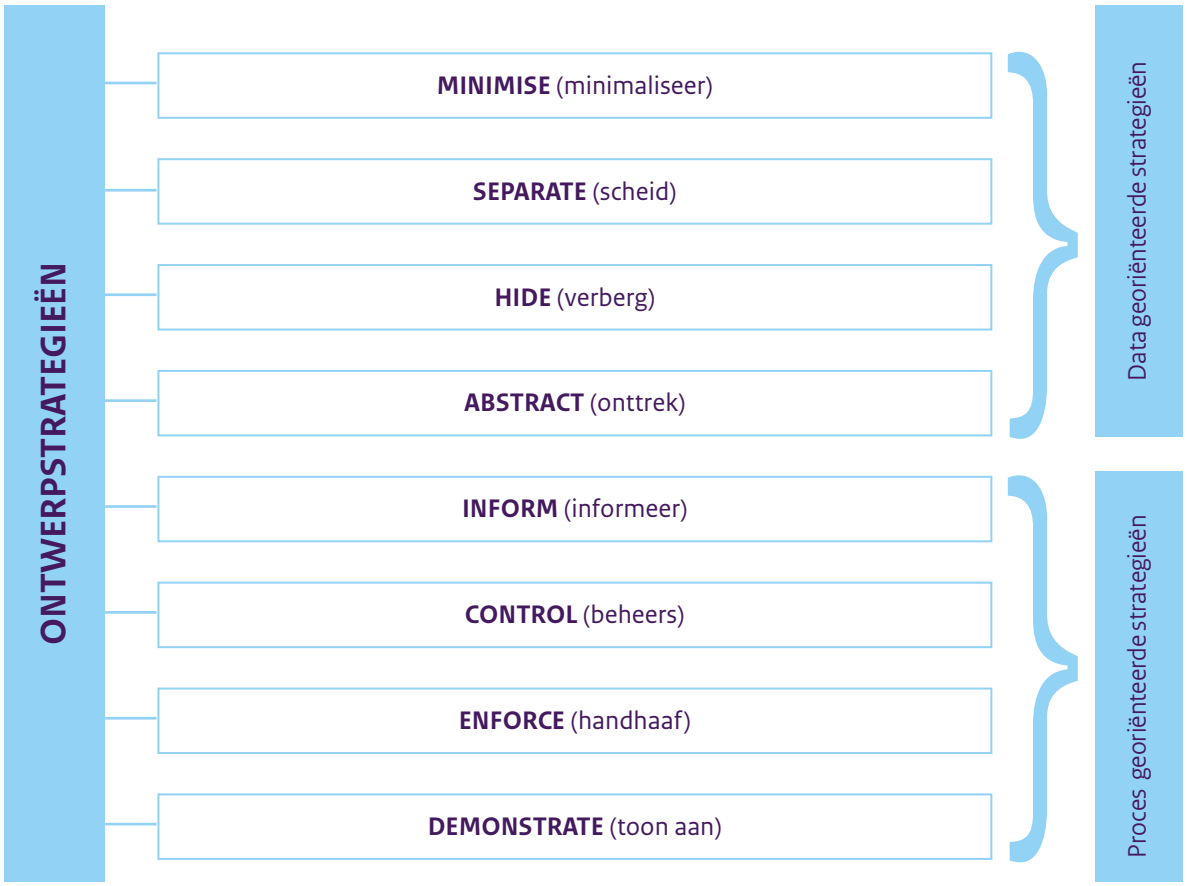
Privacy by Design (PbD) is een methode om al bij het ontwerp van een product, dienst of proces rekening te houden met het recht op privacy en gegevensbescherming. Door privacyrisico's in het ontwerp te identificeren en het ontwerp hierop aan te passen kunnen deze risico's worden vermeden.

In de *Handleiding Privacy by Design* wordt uitgelegd hoe je tot een privacyvriendelijk ontwerp komt.

5.1. Ontwerpstrategieën

Om handvatten te geven voor het doorvoeren van PbD tijdens het ontwerp en de verdere levensduur van systemen, applicaties, processen, beleid en producten, zijn een aantal **ontwerpstrategieën** ontwikkeld, neergelegd en uitgelegd in 'Het Blauwe Boekje', gratis te vinden en te downloaden hier.[30] Het gaat om de volgende ontwerpstrategieën:

Figuur 2.2. PbD data en proces georiënteerde ontwerpstrategieën.



30 De PbD 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*; Colesky, Hoepman and Hillen (2016), *A Critical Analysis of Privacy Design Strategies*; en Hoepman (2021), *Privacy is Hard and Seven Other Myths*.

De PbD ontwerpstrategieën kunnen onderverdeeld worden in **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, zoals het scheiden van databases.

De **proces georiënteerde strategieën** zijn organisatorische maatregelen. Deze maatregelen zien op de organisatie en de mens daarin. Een voorbeeld van een maatregel is het verstrekken van informatie aan betrokkenen. De proces georiënteerde strategieën zien dus niet toe op de technische maatregelen die kunnen worden getroffen.

Aan deze ontwerpstrategieën kan invulling gegeven worden door middel van een aantal tactieken (zie onderstaande tabel).

Strategie	Tactieken
Data georiënteerd	
Minimaliseer: Ziet toe op het zo veel mogelijk beperken van een verwerking van persoonsgegevens. Deze strategie draagt bij aan het beginsel minimale gegevensverwerking zoals opgenomen in artikel 5 lid 1 sub c van de AVG.	***Selecteer:*** Ziet toe op het enkel selecteren van relevante personen of persoonsgegevens. Van tevoren wordt bepaald welke gegevens relevant zijn en enkel die gegevens worden verzameld. ***Sluit uit:*** Op voorhand worden bepaalde personen of persoonsgegevens uitgesloten door van tevoren te bepalen welke gegevens of personen niet relevant zijn. ***Verwijder:*** Van tevoren wordt bepaald hoe lang persoonsgegevens nodig zijn en gegevens die niet langer nodig zijn worden verwijderd. ***Vernietig:*** Zodra persoonsgegevens niet meer nodig zijn worden ze volledig verwijderd en zijn ze niet meer beschikbaar.
Scheid: Ziet toe op het gescheiden verwerken (logisch maar ook fysiek) van verschillende persoonsgegevens. Deze strategie maakt het moeilijker verschillende gegevens te combineren.	***Isoleer:*** Verwerken van persoonsgegevens in verschillende, logisch gescheiden databases of systemen. ***Distribueer:*** Het distribueren van verwerkingen over verschillende fysieke locaties door bijvoorbeeld gebruik te maken van decentrale systemen, of de apparatuur van de eindgebruiker(s) zelf.
Verberg: Ziet toe op de vertrouwelijkheid, onherleidbaarheid en onobserveerbaarheid van persoonsgegevens.	***Beperk toegang:*** Het beperken van toegang tot persoonsgegevens door middel van toegangscontrole. ***Maak onbegrijpbaar:*** Het onleesbaar maken van persoonsgegevens door ze te versleutelen en/of te hashen. ***Verbreek link:*** Het verbreken van de link tussen persoonsgegevens en personen, bijvoorbeeld door te pseudonimiseren. ***Meng:*** Het onherleidbaar maken van persoons-gegevens door ze te mengen met andere gegevens, of door te anonimiseren.

Strategie	Tactieken
Abstraheer: Ziet toe op het zo veel mogelijk beperken van details waarin persoonsgegevens worden verwerkt.	***Groepeer:*** Het aggregeren van informatie over categorieën personen in plaats van over ieder individu afzonderlijk informatie te verwerken. ***Vat samen (generaliseer):*** Het samenvatten van gedetailleerde persoonsgegevens in meer algemene gegevens. ***Ruis toevoegen (verstoren):*** Het gebruiken van benaderingen of aanpassen van waarden in plaats van het gebruiken van de precieze waarde van een gegeven.
Proces georiënteerd	
Informeer: Ziet toe op het op tijd en adequaat informeren over de verwerking van persoonsgegevens.	***Informeer:*** Beschrijf (in een privacyverklaring) welke persoonsgegevens verwerkt worden, op welke manier en waarom. Volg de vereisten uit artikel 12, 13 en 14 AVG met het oog op transparantie over verwerkingen van persoonsgegevens. ***Leg uit:*** Beargumenteer waarom het nodig is bepaalde persoonsgegevens te verwerken en doe dit op een duidelijke en begrijpelijke manier. Informatie moet voor iedereen begrijpbaar en 'gelaagd' zijn. ***Waarschuw:*** Waarschuw gebruikers als hun persoons-gegevens gedeeld worden, gebruikt worden of deze gelekt zijn. Leg hier procedures voor vast.
Geef controle: Ziet toe op het geven van controle aan gebruikers over de verwerking van hun persoonsgegevens.	***Vraag toestemming:*** Vragen van toestemming voor de verwerking van persoonsgegevens. ***Geef keuze:*** Het geven van keuzes aan gebruikers over de verwerking en het creëren van een basismogelijkheid zonder een verwerking van persoonsgegevens. ***Corrigeer:*** Gebruikers de mogelijkheid geven om persoonsgegevens te corrigeren. ***Verwijder:*** Gebruikers de mogelijkheid geven om hun persoonsgegevens te verwijderen.
Dwing af: Ziet toe op het intern dwingen binnen een organisatie om persoonsgegevens op een privacy vriendelijke manier te verwerken.	***Stel vast:*** Committeer je als organisatie aan privacy middels een privacybeleid, en stel doelen op en middelen beschikbaar om dit uit te voeren. ***Dwing af:*** Het afdwingen van beleid door maatregelen te implementeren en verantwoordelijkheden te beleggen. ***Beheer:*** Het regelmatig controleren van beleid en de implementatie daarvan.
Toon aan: Ziet toe op het aantonen van en privacy vriendelijke wijze van het verwerken van persoonsgegevens.	***Leg vast:*** Het documenteren van de belangrijke stappen die je neemt en vastleggen van beslissingen. ***Audit:*** Het auditen van verzamelde logs maar ook het auditen van de manier van werken en verwerken van persoonsgegevens. ***Rapporteer:*** Het rapporteren van resultaten van audits en overleggen over bepaalde resultaten met bijvoorbeeld een toezichthouder.

September 2024 | Publicatie-nr. 24407665