Actieplan Privacy

Eindrapportage

Datum:	13 november 2014
Auteurs:	Arnold Roosendaal, Marc van Lieshout, Colette Cuijpers, Ronald Leenes.
Opdracht:	Deze opdracht is uitgevoerd door het Privacy & Identity Lab in opdracht van het Ministerie van Economische Zaken. Deze opdracht is uitgevoerd onder de in de offerte genoemde voorwaarden. Aanbiedingsbrief: 2012-MII-344-FvA-NvB Offertenummer: 900797
Penvoerder:	Penvoerder voor deze opdracht namens het Privacy & Identity Lab: TNO.
Rapportnummer:	TNO 2014 R11603

Dit rapport is geschreven door het Privacy & Identity Lab en vertegenwoordigt niet het standpunt van de Minister van EZ. De Radboud Universiteit, TNO, Tilburg University en SIDN, het bedrijf achter.nl, werken gezamenlijk aan betere oplossingen voor het beheren van online privacy en elektronische identiteiten. Daartoe hebben ze het Privacy & Identity Lab opgericht, een expertisecentrum waarin ze bestaand onderzoek bundelen en nieuw onderzoek opzetten. Het samenwerkingsverband is uniek, omdat het de technische, juridische en socio-economische aspecten van privacy en identiteit integraal onderzoekt.

Managementsamenvatting

De aandacht voor privacybescherming van burgers en consumenten is onverminderd hoog. Een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer draagt bij aan het digitale vertrouwen van betrokkenen en daarmee aan de groei van digitale diensten. Er zijn zeker kansen voor innovatie in digitale diensten waarbij privacy geborgd is. De kennis hierover en inzichten over de wijze waarop dat kan is echter niet altijd aanwezig. Het Actieplan Privacy heeft dit hiaat zichtbaar gemaakt en doet suggesties om dit op te vullen.

In de eerste fase van het Actieplan Privacy is desk research uitgevoerd om een overzicht te verkrijgen van best technologies en best practices op het gebied van privacy innovatie. Hoofdstuk 2 van dit eindrapport geeft hier een korte weergave van. Er zijn drie hoofdcategorieën waarbinnen de best technologies en best practices ingedeeld zijn: Oplossingen voor het verbeteren van diensten; Oplossingen voor het verbeteren van netwerken van organisaties en individuen, en; Oplossingen voor het versterken van de positie van het data subject. Het volledige overzicht toont aan dat er een breed assortiment aan technologies en practices voorhanden is. In veel gevallen vinden deze echter nog niet de weg van een academische setting naar een praktische implementatie. De tweede fase van het Actieplan Privacy was er daarom op gericht om de praktijk verder te brengen.

Ten eerste is er gekeken naar enkele praktijkvoorbeelden waar privacy als innovatie goed geslaagd is. In hoofdstuk 3 wordt eerst beschreven hoe CV-OK met de dienst YOPS (Your Online profile Safe) een niche heeft ontdekt en een privacyvriendelijke dienst aanbiedt, waarbij de controle over gegevens zoveel mogelijk bij het data subject wordt gelegd. Door de faciliteit van een digitale kluis met geverifieerde gegevens wordt tevens het aantal verwerkingen en uitvragingen van verschillende instanties gereduceerd, terwijl de gegevens toch betrouwbaar blijven. Vervolgens zijn enkele initiatieven van NS beschreven, waarbinnen privacy een belangrijke rol speelt. Zo worden diensten verleend waarbij alleen reizigersaantallen worden geteld met behulp van infrarood, waardoor geen persoonsgebonden informatie verwerkt hoeft te worden. In andere gevallen, waar het wel noodzakelijk is om persoonsgegevens te verwerken, is dataminimalisatie het leidende principe geweest.

In een consultatieworkshop met ruim 40 deelnemers van diverse achtergronden (bedrijfsleven, consultancy, wetenschap, beleidsmakers, brancheorganisaties) is een aantal praktijken gepresenteerd. De voorbeelden werden als inspirerend ervaren, maar desondanks bleek het voor veel partijen nog niet eenvoudig om privacy in de bedrijfsvoering in te bedden. Een drietal invalshoeken bleek van belang. Allereerst is er het juridisch kader voor gegevensbescherming dat vaak als complex wordt ervaren en als een belemmerende factor voor innovatie. Ten tweede wordt er binnen branches veel naar collega bedrijven gekeken en spelen vergelijkbare vragen of belemmeringen voor meerdere partijen binnen die branches. Ten derde blijkt dat privacy lang niet altijd hoog op de agenda staat binnen bedrijven en is het geen standaard onderdeel van de dagelijkse gang van zaken.

Het juridische kader heeft echter ook een bepaalde innovatieve kracht (hoofdstuk 4). In een expert workshop kwam een aantal factoren op tafel dat vanuit juridisch perspectief een rol speelt. De complexiteit van het kader werd erkend, maar tegelijkertijd werd aangegeven dat regulering ook kansen biedt en bedrijven juist uitdaagt tot innovatieve oplossingen. De aankomende Algemene Verordening Gegevensbescherming zal dat naar verwachting alleen maar versterken. Op het gebied

van juridische consultancy is al een redelijk volwassen markt ontstaan. Privacy wordt soms gezien als differentiator en er wordt ook geanticipeerd op de aankomende Verordening. Het belang van regelgeving is ook duidelijk: het biedt een kader waar bedrijven zich naar zullen moeten schikken.

De andere twee invalshoeken liggen meer binnen de mogelijkheden van bedrijven om invloed op uit te oefenen. Brancheorganisaties (hoofdstuk 5) kunnen een verbindende rol spelen tussen bedrijven, maar kunnen er ook voor zorgen dat informatie en kennis goed verspreid worden onder de achterban. Op dit moment is er een aantal voorbeelden van waar dat goed gebeurt, bijvoorbeeld in de vorm van praktische handleidingen en symposia. Er is echter in veel gevallen nog ruimte voor een actievere opstelling van brancheorganisaties. Naast het verspreiden van kennis en het verbinden van bedrijven kunnen brancheorganisaties meewerken aan het uitdragen van privacy als kans voor innovatie. Er is dus behoefte aan positieve communicatie en het bieden van een platform aan inspirerende voorbeelden. Enkele voorlopende bedrijven kunnen de kar gaan trekken, maar een branche-brede aanpak is effectiever en kan sneller tot draagvlak leiden.

Binnen bedrijven zelf liggen ook mogelijkheden (hoofdstuk 6). Het gaat dan immers om de interne huishouding. Wanneer privacy goed op de agenda wordt gezet en in alle lagen van het bedrijf wordt geborgd wordt het uiteindelijk een vanzelfsprekendheid. Het idee binnen bedrijven moet veranderen van privacywetgeving als een belemmerende factor waardoor innovatie teruggefloten wordt, naar privacywetgeving als een uitdagend kader waar innovatief goed mee gewerkt kan worden. Zeker binnen grotere bedrijven kan een functionaris voor de gegevensbescherming of een Privacy Officer daar een belangrijke rol in spelen. De aanstelling van een dergelijk persoon zorgt voor waarborgen op het gebied van compliance. Voorwaarde is wel dat de functie vanuit het hoger management ondersteund wordt met concrete bevoegdheden.

Vanuit verschillende invalshoeken zijn er dus kansen voor het verder brengen van privacy als innovatie. De rol van privacy als kans binnen bedrijven kan drie vormen aannemen:

1. Privacy als service enabler
2. Privacy als niche
3. Privacy als compliance factor

Tenslotte moet er rekening mee gehouden worden dat er een categorie bedrijven is waar het business model gebaseerd is op verwerking van persoonsgegevens en waar dus helemaal geen incentive is om privacy vriendelijk te innoveren. Met name voor deze categorie blijft het regelgevend kader en handhaving van belang.

Uit het onderzoek volgt een zevental aanbevelingen voor het stimuleren van privacy vriendelijke innovatie binnen Nederland. Deze liggen op het gebied van

1. **Bij elkaar brengen van partijen** met als doel een systematische monitoring van privacy-praktijken, het vergroten van de *awareness* voor deze praktijken in de buitenwereld, en het delen en verspreiden van kennis en ervaringen over invoering van privacy-praktijken.
2. **Nieuwe kennisontwikkeling** rond privacy met het oog op innovatieve oplossingen die economisch en maatschappelijk renderen.

3. **Opstellen van een privacy benchmark** om duidelijke richtlijnen te bieden met betrekking tot inbedding van privacy in bedrijfsvoering. Daarnaast ontwikkeling van bewustwording en standaarden.
4. **Ondersteunen van innovatieve start-ups** om kansen om nieuwe privacydiensten en –producten te vervolmaken en te vermarkten te verhogen. Daarmee wordt ook de aantrekkelijkheid voor start-ups om zich in deze markt te begeven vergroot.
5. **Organiseren van een Privathon** om onderzoekers te betrekken bij het vinden van oplossingen voor specifieke privacyvraagstukken en om de mogelijkheden om dit met technische oplossingen verder te brengen onder de aandacht te brengen.
6. **Voorbeeldfunctie overheid**: 'Practice what you preach'. Stimuleer rijksbrede bewustwording van mogelijkheden voor privacyvriendelijke innovatie.
7. **Algeheel compliance en beschermingsniveau verhogen** om privacybescherming te bevorderen.

Inhoudsopgave

1 Inleiding

De aandacht voor privacybescherming van burgers en consumenten is onverminderd hoog. In de Monitor ICT, Veiligheid en Vertrouwen 2012 door TNO[1] is bezorgdheid om privacy de meest genoemde reden voor consumenten om van het gebruik van een dienst op internet af te zien. Zoals het in de recente kabinetsbrief aan de Tweede Kamer over e-Privacy gesteld wordt: een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer draagt bij aan het digitale vertrouwen van betrokkenen en daarmee aan de groei van digitale diensten.[2]

Privacy biedt kansen voor innovatie, en vormt soms een barrière voor internetdiensten. Er is en wordt veel technologie ontwikkeld die uitzicht biedt op slimme privacy-vriendelijke oplossingen in bedrijfsprocessen. Kansen liggen er niet alleen in het toepassen van deze oplossingen waarmee risico's vermeden worden en de zorg om privacy als een *unique selling point* kan gelden, maar ook in het verder ontwikkelen en vermarkten van deze oplossingen. Technologie maakt in dat geval nieuwe diensten mogelijk: privacy is dan een *service enabler*. Een voorwaarde voor het grijpen van deze kansen is dat er voldoende kennis over aanwezig moet zijn bij bedrijfsleven en publieke organisaties, en inzicht in de mogelijkheden die de oplossingen kunnen bieden. Juist deze kennis en dit inzicht is niet altijd aanwezig.

Het Actieplan Privacy heeft als doelstelling dit hiaat op te vullen, en daarmee de belangrijke dienstensector in Nederland tot privacy-vriendelijke innovatie te stimuleren zodat ze zich daarmee op het gebied van privacy een vooraanstaande positie kan verschaffen.

Dit is het eindrapport van het Actieplan Privacy dat door het PI.lab is uitgevoerd in opdracht van het Ministerie van Economische Zaken. Het bevat een verslag van de tweede fase van het project. In de eerste fase is desk research uitgevoerd om te komen tot een inventarisatie van Best Practices en Best Technologies voor privacy-vriendelijke innovatie. Dit desk research is in een eerste rapport uitgewerkt (Annex 3). Hierin is duidelijk geworden dat er meer technologieën en praktijken voorhanden zijn dan vaak op het eerste gezicht wordt gedacht. De resultaten van de eerste fase zijn gepresenteerd in een consultatieworkshop met deelnemers uit bedrijfsleven, overheid en brancheorganisaties. Na de consultatieworkshop is een aantal innovatiepraktijken in gang gezet om privacy-vriendelijk innoveren daadwerkelijk een stap verder te brengen. Dit rapport geeft een verslag van deze innovatiepraktijken. Daarnaast is, op basis van de bevindingen uit de consultatieworkshop, tevens aandacht besteedt aan enkele andere factoren die een belangrijke rol kunnen spelen in het tot stand brengen van privacy-vriendelijke innovatie. Allereerst gaat er een innovatieve kracht uit van regulering. Door strenge wettelijke kaders wordt immers een beroep gedaan op de innovatieve kracht van bedrijven om daar goed mee om te gaan, zonder dat de dienstverlening in het gedrang komt. Ten tweede is er een belangrijke rol weggelegd voor brancheorganisaties, met name op het gebied van voorlichting en ondersteuning op branche-niveau. Ten derde blijkt een goede privacy-officer (Functionaris voor de Gegevensbescherming) een essentiële rol te kunnen vervullen. Privacy-vriendelijke innovaties zijn dus niet alleen afhankelijk van de beschikbare technologie, maar ook van het privacyklimaat binnen een bedrijf of branche.

[1] TNO, 2012, Monitor ICT, Veiligheid en Vertrouwen.

[2] Ministerie van Economische Zaken, Brief Kabinetsvisie op e-privacy: op weg naar gerechtvaardigd vertrouwen, 24 mei 2013

Er is dus een aantal factoren die een rol kunnen spelen in privacy innovatiepraktijken. Vaak wordt eerst gedacht aan beveiliging van gegevens. Daarmee wordt echter slechts aan een deel van de vereisten uit de wetgeving voldaan. Verdere stappen vergen echter extra inspanning. Het is in de workshops gebleken dat er vanuit verschillende organisaties absoluut de wil is om te innoveren en om privacy en gegevensbescherming in de organisatie te verbeteren. Een aantal bedrijven wil privacy zelfs als onderscheidende factor gebruiken ten opzichte van concurrentie. Er is een groot bewustzijn van het belang van privacy en daarmee zijn er ook kansen om technologisch en organisatorisch vooruitgang te boeken. Het Actieplan Privacy heeft als doel daaraan bij te dragen door te werken aan bekendheid met bestaande technologieën en praktijken, dialoog met bedrijfsleven en brancheorganisaties en het ondersteunen van een aantal privacy innovatiepraktijken. Bovendien is een aantal andere factoren die bij kunnen dragen aan het verbeteren van privacybescherming belicht.

1.1 Doel van dit actieplan

Het Actieplan Privacy heeft als doelstelling om de belangrijke dienstensector in Nederland zodanig tot privacy-vriendelijke innovatie te stimuleren dat ze zich een vooraanstaande positie kan verschaffen binnen Europa en daarbuiten.

1.2 Aanpak

In het desk research in de eerste fase van het Actieplan Privacy is zowel gekeken naar *best practices* op het gebied van technologie en ontwerp van informatiesystemen als naar *best practices* bij het inrichten van een organisatie. De selectie van *best practices* voor de inventarisatie heeft plaatsgevonden aan de hand van een aantal criteria. De technologieën en werkwijzen of modellen die werden beschreven:

(1) beschermen de privacy,

(2) hebben zich in meer of mindere mate bewezen in de praktijk en

(3) bieden bedrijven een kans om te innoveren.

Het desk research bestond uit drie stappen:

(1) de breedte verkennen door het opstellen van een lijst van *best practices*;

(2) een beperkte verdieping door uitwerken van de *best practices* van de lijst tot korte omschrijvingen; en

(3) een analyse van de resultaten van het desk research. Tijdens de analyse zijn de best practices gegroepeerd in ‘constellaties’ van technologieën en praktijken die in samenhang een systeemoplossing bieden.

Bronnen die gebruikt zijn rapporten en projecten die zijn uitgevoerd door het PI.lab (TNO, Radboud Universiteit Nijmegen en TILT), relevante wetenschappelijke publicaties en voorbeelden die zijn gepresenteerd tijdens conferenties, de open onderzoeksdatabase SSRN, en een brainstorm onder de deelnemers van het PI.Lab. Bij de korte omschrijvingen van *best practices* wordt verwezen naar enkele kernpublicaties or bronnen die de geïnteresseerde verder kunnen helpen.

De uitgewerkte *best practices* zijn niet allemaal direct toepasbaar; privacybescherming is een domein wat sterk in ontwikkeling is, waardoor juist kansen voor innovatie ontstaan. Op basis van de resultaten uit het desk research is een consultatiesessie gehouden met stakeholders in Nederland, om te onderzoeken welke kansen zij zien voor de technologieën en werkwijzen voor de innovatie in Nederlandse bedrijven. Bij de consultatie waren zowel grote als kleine bedrijven vertegenwoordigd. Daarnaast waren er beleidsmakers van verschillende ministeries, brancheorganisaties, Functionarissen voor de Gegevensbescherming en enkele consultants aanwezig.

Na de consultatiesessie is in samenwerking met enkele bedrijven gekeken naar privacy innovatiepraktijken. Dit betreft YOPS (Your Online Profile Safe), een dienst opgezet door CV-OK, die het mogelijk maakt om online CV's inclusief geverifieerde documenten te beheren en in de controle van het individu te houden, en een aantal innovaties bij NS, waar privacy een centrale rol speelt. Daarnaast is veel met verscheidene bedrijven gesproken en zijn in dit rapport nog andere illustrerende voorbeelden opgenomen.

Omdat tijdens de consultatie duidelijk naar voren kwam dat brancheorganisaties en Functionarissen voor de Gegevensbescherming een belangrijke rol kunnen spelen is hieraan ook nog specifiek aandacht besteed in dit rapport. Tevens is een hoofdstuk gewijd aan de innovatieve kracht van privacyregulering. De inhoud van dat hoofdstuk is mede gebaseerd op een workshop die in het kader van dit Actieplan is georganiseerd, specifiek op dat deelonderwerp.

1.3 Leeswijzer

Dit rapport kan als volledig eindrapport van het Actieplan Privacy gelezen worden. Van het eerste deel, het desk research, is een apart rapport verschenen. Voor de leesbaarheid is daarvan een samenvattend overzicht opgenomen in dit rapport in hoofdstuk 2. Indien u reeds bekend bent met het eerste rapport kunt u dit hoofdstuk dus overslaan. Voor de volledigheid is het rapport van het desk research integraal bij dit rapport gevoegd (Annex 3).

Vervolgens worden de innovatiepraktijken en overige invalshoeken besproken. Het hoofdstuk over de innovatieve kracht van regelgeving is gebaseerd op de resultaten uit een workshop met experts. Deze workshop werd ingeleid door een aantal pitches. Een verslag van deze pitches is bij dit rapport gevoegd in Annex 1. Een uitgebreidere weergave van de workshop is te vinden in Annex 2.

2 Best Practices en Best Technologies voor privacy innovatie

Privacy innovatie kan gebaseerd zijn op twee pijlers: een organisatorische insteek en een technologische insteek. Voor beide aanpakken zijn er al verschillende voorbeelden beschikbaar, die in meer of mindere mate ook hun weg naar de praktijk hebben gevonden. In het eerste deel van het Actieplan Privacy is een desk research uitgevoerd om een overzicht samen te stellen van Best Practices en Best Technologies op het gebied van privacy innovatie. Hier wordt een beknopte weergave gegeven van de resultaten uit het desk research. Een integrale versie van het rapport betreffende het desk research is opgenomen in Annex 3 bij dit rapport.

2.1 Ordening van geïdentificeerde best practices en best technologies

De geïdentificeerde *best technologies* en *best practices* die, veelal in combinaties en in samenhang, een oplossing kunnen bieden, zijn geordend aan de hand van het op te lossen probleem. Daaruit ontstaan drie categorieën van oplossingen. Allereerst zijn er een aantal oplossingen die gericht zijn op het verbeteren van diensten. Daaronder vallen vanuit technologisch perspectief ontwerpen voor privacy, dus technologieën die gericht zijn op het borgen van privacy binnen een dienst. Voorbeelden hier van zijn Privacy by Design - Privacy Design Strategies - Privacy Design Patterns - Privacy Enhancing Technologies - Userinterface ontwerp voor privacy - Anonimisering en pseudonimisering - Anonymous credentials - Standaarden voor informatiebeveiliging. Vanuit organisatorisch perspectief kunnen daar een aantal oplossingen toegevoegd worden die privacy binnen processen en de organisatie als geheel borgen. Het gaat dan bijvoorbeeld om Privacy Impact Assessments - Privacy Maturity Model - Functionaris gegevensbescherming - Training en bewustzijn.

Een tweede categorie oplossingen is gericht op het verbeteren van netwerken van organisaties en individuen. Hier zijn vooral technische benaderingen te vinden die vertrouwensnetwerken mogelijk maken, zoals een Digitale gegevenskluis - Sticky policies - Context-aware privacy policies.

De derde categorie oplossingen legt de nadruk op het versterken van de positie van het data subject. Een combinatie van technische en organisatorische oplossingen is gericht op geïnformeerde toestemming, bijvoorbeeld door het gebruik van Toegankelijke privacy statements - Ondersteunen van het 'recht om vergeten te worden' - Gelaagde toestemming – Persoonsgegevensdashboard - Access logs. Daarnaast zijn er een aantal technische tools om de zelfredzaamheid van het data subject op het gebied van privacybescherming te vergroten. Daarbij kan gedacht worden aan Transparantietools - Private browsing - Do Not Track - Versleuteling van opgeslagen persoonsgegevens - Onion Routing - Proxy servers.

De verschillende categorieën en bijbehorende *best practices* en *best technologies* worden hieronder nader uitgewerkt.

2.2 Oplossingen voor het verbeteren van diensten

De oplossingen voor het verbeteren van diensten zijn onder te verdelen in ontwerpen voor privacy en het inrichten van processen en de organisatie. Beiden worden hieronder nader uitgewerkt.

2.2.1 Ontwerpen voor privacy

Als een onderneming een bedrijfsproces aan wil passen of een nieuw product of dienst op de markt wil brengen, biedt dit mogelijkheden om ook na te denken over de privacyaspecten hiervan.

Inmiddels zijn er verschillende instrumenten beschikbaar om deze privacyaspecten van meet af aan mee te nemen in het ontwerpproces. Privacy by Design, Privacy Design Strategies en Privacy Design Patterns vormen een drieluik dat loopt van het ontwerp tot de concrete implementatie van een privacy-vriendelijke oplossing. Privacy by Design geeft het raamwerk en de functionele eisen waaraan een systeem moet voldoen, Privacy Design Strategies maken het mogelijk om bepaalde accenten te leggen (zoals segregatie van gegevensstromen, of minimalisatie van gegevensverzameling) en Privacy Design Patterns bieden de technische vertaling van de strategieën.

Voor minimale herkenbaarheid van personen en maximale beveiliging van persoonsgegevens kan gekozen worden voor anonimisering of (minder vergaand) pseudonimisering van gegevens. De keuze hiervoor zal ingegeven worden door de gekozen mate van privacyvriendelijkheid. Anonymous credentials bieden de mogelijkheid om diensten aan te bieden waar zo weinig mogelijk identificerende gegevens voor nodig zijn (zoals het gebruik van leeftijdsverificatie voor het verkopen van drank of games). Aan de beveiligingskant is een palet aan standaarden beschikbaar die de informatiebeveiliging regelen.

2.2.2 Inrichten van processen en organisaties

Naast het bieden van technische oplossingen is een belangrijke rol weggelegd voor organisatorische en procesmatige aanpakken. Technologie alleen is onvoldoende om tot breed gedragen privacyvriendelijke oplossingen te komen. Voor de uitvoering van een *Privacy Impact Assessment* – het op een systematische en gestructureerde manier in kaart brengen van privacyrisico's die aan een nieuw proces, dienst of product kleven en het aanbieden van manieren om deze risico's waar gewenst aan te pakken – zijn inmiddels verschillende bedrijven en organisaties in te schakelen. Een organisatie kan zich zelf een doel stellen in het omgaan met privacy en kan streven naar een bepaalde mate van maturiteit. Het *Privacy Maturity Model* geeft aan hoe die maturiteit te bepalen is door te kijken naar de wijze waarop bepaalde maatregelen al dan niet structureel en systematisch in een organisatie zijn verankerd. In sommige gevallen is het verplicht om een *Functionaris Gegevensbescherming* (publieke organisaties) of een *Privacy Officer* (publieke en private organisaties) aan te stellen, een onafhankelijk persoon binnen de organisatie die toeziet op naleving van privacyvereisten. *Training en bewustzijn vergroten* binnen een organisatie draagt bij aan de structurele verankering van privacybewustzijn en manieren van omgaan met persoonsgegevens.

2.3 Oplossingen voor het verbeteren van netwerken van organisaties en individuen

2.3.1 Vertrouwensnetwerken

Door verschillende partijen wordt gewerkt aan het bieden van trusted architectures en trusted services. Door gebruik te maken van verschillende beveiligings- en verantwoordingselementen in het netwerk kan een end-to-end secure systeem worden aangeboden. Deze netwerken kunnen centraal georganiseerd zijn (one2many) waarbij regels en procedures over de omgang met persoonsgegevens centraal (contractueel) worden vastgelegd. Daarnaast zijn er multi-stakeholder netwerken (many2many) die verschillende partijen verenigt onder een set van afspraken en procedures. Ook in Nederland zijn er inmiddels voorbeelden van beide vormen te vinden.

De vertrouwensnetwerken kunnen gebruik maken van maatregelen zoals een digitale gegevenskluis, sticky policies en context-aware privacy policies. Een digitale gegevenskluis geeft de controle over de

opgeslagen gegevens terug aan de eigenaar van de gegevens. De procedures zijn zodanig geregeld dat de eigenaar kan beslissen of en voor welk doel gegevens beschikbaar worden gesteld. Door gebruik van sticky policies kan softwarematig geregeld worden dat bepaalde vormen van gebruik van persoonsgegevens onmogelijk wordt gemaakt. Context-aware privacy policies zijn privacy policies die zodanig zijn opgesteld dat gebruik en beheer van gegevens afhankelijk is gemaakt van de context van gebruik. Aan de koppeling van context-aware privacy policy systemen wordt gewerkt. Het is duidelijk dat dit geen eenvoudige zaak is omdat de context specifiek vertaald moet worden in toegestane bewerkingen.

2.4 Oplossingen voor het versterken van de positie van het datasubject

Een derde perspectief op het ontwerpen en beheren van privacyvriendelijke oplossingen richt zich op het datasubject van wie gegevens verzameld, bewerkt, gebruikt en verspreid worden. De digitale kluis die onder het vorige kopje is genoemd, maakt ook onderdeel uit van de maatregelen die hier getroffen kunnen worden. We onderscheiden twee invalshoeken. Ten eerste: in hoeverre is het mogelijk het datasubject te betrekken bij de aard van de gegevensverzameling en het gebruik ervan? Geïnformeerde instemming is hier het sleutelwoord. En ten tweede: in hoeverre kan het datasubject middelen worden geboden die het mogelijk maken een sterkere controle uit te oefenen over zijn of haar persoonsgegevens? Ook hier zijn verschillende tools voor beschikbaar.

2.4.1 Geïnformeerde toestemming

Eén van de mogelijke grondslagen voor legitieme verzameling en bewerking van persoonsgegevens is de toestemming van de persoon wiens gegevens het betreft. Deze toestemming moet aan een aantal voorwaarden voldoen. Zo moet helder zijn waarvoor toestemming gegevens wordt, voor welke doeleinden, en welke gegevens het betreft. Via transparante en leesbare privacy statements kan het datasubject geïnformeerd worden welke gegevens met welk doel verzameld worden. Het schrijven van bondige en informatieve policy statements is een vak apart. Er zijn middelen op de markt die het opstellen van deze statements ondersteunen. Ook het bieden van een gelaagde toestemming in plaats van een ‘alles of niets’ benadering kan helpen bij het verder verfijnen van de toestemmingsvereisten. Via een privacy dashboard kan een datasubject in één oogopslag zien welke gegevens voor welke dienst benut worden en welke privacyrisico’s daar aan verbonden zijn.

2.4.2 Zelfredzaamheid in privacy

Private browsing en Do not track zijn technieken die het onmogelijk maken om navigatiesessies te volgen. Door systematische toepassing van versleutelingstechnieken kan een datasubject waarborgen inbouwen in het afschermen van zijn gegevens. Het gebruiken van Onion routers en proxy servers maakt het onmogelijk om verkeersstromen te volgen en te zien welke route gegevens afleggen. Transparantietools, tot slot, werken de andere kant op en maken inzichtelijk voor het datasubject welke gegevens verzameld worden.

3 Innovatiepraktijken

Het desk research heeft een overzicht opgeleverd van bestaande technologieën en praktijken om privacy beter te beschermen. Om deze best practices en best technologies daadwerkelijk hun waarde te laten hebben is echter wel vereist dat ze ook in de praktijk worden toegepast. Het gaat in feite om twee stappen: allereerst dient er bekendheid te zijn met de voorhanden zijnde oplossingen en vervolgens moeten de oplossingen praktisch ingezet worden door organisaties. Hoewel vaak gedacht wordt dat organisaties niet graag in privacy willen investeren lijkt het in de praktijk eerder om onwetendheid te gaan. Er is absoluut de wil om privacy beter te beschermen. Dat bleek ook uit de diversiteit van de ruim 40 deelnemers aan de consultatiesessie. Voor veel partijen is het echter de vraag hoe privacy beter geborgd kan worden.

Gedurende de consultatiesessie is een aantal inspirerende praktijkvoorbeelden gepresenteerd. Deze voorbeelden dienden tevens als aanzet voor discussie over de haalbaarheid en aanpak van privacy-innovatie. Vervolgens is met enkele andere partijen aan privacy-innovatiepraktijken gewerkt. Deze innovatiepraktijken worden in dit hoofdstuk nader beschreven.

3.1 Your Online Profile Safe (YOPS)

Er is behoefte aan het verifiëren van de juistheid van gegevens in CV's van kandidaten voor een baan. Als werkgever wil je immers zeker weten dat een werknemer bepaalde kwalificaties heeft. In beginsel gaat het dan vooral over diploma's en werkervaring. Daarnaast kunnen echter specifieke gevallen aan de orde zijn, zoals VOG-verklaringen (Verklaring omtrent gedrag), een check op een strafrechtelijk verleden en eventuele faillissementen. In voorkomende gevallen is de werkgever daartoe zelfs wettelijk verplicht. Het belang van een goede check en de gegevens die in een screening meegenomen moeten worden hangt samen met de functie waarvoor iemand solliciteert en bij wat voor type organisatie. Om aan de behoefte van werkgevers aan screenings en controle van CV's te voldoen is in 2009 CV-OK opgericht. CV-OK levert een software oplossing voor employment screening.

In het verlengde van de dienstverlening rondom CV-OK is een nieuwe innovatie gaande, YOPS. YOPS staat voor Your Online Profile Safe en is voornamelijk gericht op ZZP-ers, gedetacheerden, consultants en uitzendkrachten die herhaaldelijk van baan wisselen. Het gaat dus om flexwerkers (de flexschil). Het model is hier omgedraaid: niet de werkgever betaalt voor een screening, maar de werknemer betaalt voor het onderhouden van zijn of haar geverifieerde gegevenskluis.

3.1.1 De diensten van CV-OK

CV-OK werd opgericht in 2009 om een software oplossing voor employment screening te bieden aan werkgevers. De screenings verifiëren de gegevens die een kandidaat in zijn of haar CV heeft opgenomen. Daarbij gaat het bijvoorbeeld om behaalde diploma's, VOG verklaringen en werkervaring. Ook kan gekeken worden of iemand een strafrechtelijk verleden heeft of bepaalde schulden. De dienst is modulair opgebouwd en per screening kan aangegeven worden welke onderdelen geverifieerd dienen te worden. Voor iemand die solliciteert naar een functie als receptioniste zal bijvoorbeeld geen financiële screening op faillissementen en schulden vereist zijn, maar voor een functie als financieel directeur wel. Door de modulaire opbouw kan op deze wijze ook voldaan worden aan de proportionaliteit en subsidiariteit van de screening, zoals vereist in de Wbp.

Er wordt niet meer gescreend dan noodzakelijk voor het beoogde doel in relatie tot de functie waar het in het individuele geval om gaat.

Er worden twee typen screenings aangeboden.

1. Pre-employment: voorafgaand aan dienstverband
2. In-employment: periodiek tijdens dienstverband

Voor het verifiëren van de gegevens werkt CV-OK samen met een aantal data leveranciers. Daaronder bevinden zich onder meer Dienst Uitvoering Onderwijs (DUO), ID Checker, Focum en Nuffic.

CV-OK is een zelfstandige organisatie. Ook al zijn werkgevers opdrachtgever voor de screenings, CV-OK is zelf een verantwoordelijke in de zin van de Wet bescherming persoonsgegevens (Wbp). De partners waarmee CV-OK samenwerkt om de screenings uit te voeren zijn bewerkers en verwerken de specifieke gegevens op basis van een bewerkersovereenkomst. In het geval van DUO wordt zelfs rechtstreeks in de systemen van CV-OK gewerkt. De kandidaat geeft aan wat de inschrijvings- en uitschrijvingsjaren waren en of het diploma inderdaad behaald is. Het systeem van CV-OK vraagt bevestiging aan DUO, DUO voert de controle in hun eigen systeem uit en bevestigt de gegevens in het systeem van CV-OK.

CV-OK geeft als uitkomst van de screening een overzicht van de geverifieerde onderdelen. Daarbij zit uitdrukkelijk geen advies of risico-analyse omtrent de kandidaat en/of zijn of haar omgeving. Voor dergelijke risico-analyses is vereist dat een organisatie een vergunning heeft voor recherchewerk, wat bij CV-OK niet het geval is. Het doel is ook niet om te oordelen, maar om te verifiëren. Een werkgever moet uiteindelijk zelf beslissen of hij met een kandidaat in zee gaat.

Werkgevers kijken vaak ook naar profielen van kandidaten op sociale media alvorens een kandidaat wordt uitgenodigd voor een gesprek. De gedragscode voor HR-personeel (NVP Sollicitatiecode) schrijft voor dat hier zorgvuldig mee omgegaan dient te worden. Naast het feit dat de informatie die op profielen te vinden is wellicht niet relevant is voor het functioneren van de kandidaat, is het ook mogelijk dat een verkeerd profiel wordt bekeken. Vaak zijn er tenslotte meerdere mensen met dezelfde naam en het gebruik van eventuele pseudoniemen bemoeilijkt het vinden van de juiste persoon. Teneinde meer zekerheid te bieden kan CV-OK als onderdeel van de screening het ‘Internet Profiel’ leveren – dat is een overzicht van de url’s van de persoon. Voordeel voor de opdrachtgever is dat het 1) tijd bespaart, 2) je weet zeker dat je ook voldoet aan de NVP Sollicitatiecode (nl de kandidaat is van tevoren ingelicht) en 3) je weet zeker dat je naar de juiste persoon kijkt, en dus niet naar een naamgenoot. Dat staat overigens los van het advies om profielen af te sluiten voor buitenstaanders door verstandig gebruik van de privacy-instellingen van een sociale netwerk site. Er is dus meer controle en transparantie over het bekijken van profielen op sociale media. Desalniettemin blijft de legitieme grondslag voor verwerking hier een lastig punt. Vanwege het aanleveren van de gegevens door de kandidaat lijkt er sprake te zijn van geïnformeerde toestemming. Omdat er echter sprake is van een afhankelijkheidsrelatie (potentieel werkgever-werknemer) kan niet gesteld worden dat de kandidaat de gegevens volledig uit vrije wil verschaft. Daarmee vervalt deze grondslag. De juiste grondslag voor de verwerking van persoonsgegevens is in dit geval 8(f): het gerechtvaardigd belang van de opdrachtgever die een screening moet laten

uitvoeren om aan wettelijke eisen te voldoen. Een zorgvuldig beleid vereist daarbij dat proportionaliteit en subsidiariteit in acht worden genomen. De toestemming van de kandidaat is wel vereist voor het opvragen van inzage in de databanken van DUO (IB-groep) voor checks van diploma's etc. Tevens vragen referenten vaak naar een vorm van toestemming. Met het vragen om toestemming en de vrijwillige basis voor het aanleveren van sociale netwerk informatie wordt invulling gegeven aan proportionaliteit en subsidiariteit bij het afwegen van de belangen.

In het business model van CV-OK verzoekt een werkgever om een screening. De werkgever betaalt aan CV-OK een vergoeding voor de uitvoering van de screening. De hoogte van de vergoeding is afhankelijk van welke onderdelen gescreend worden. De werkgever en kandidaat gaan normaal gesproken een arbeidsrelatie voor langere tijd aan. Daarmee staan de kosten ook in verhouding tot de samenwerking. Er zijn echter ook steeds meer ZZP-ers, flexwerkers en interim werknemers. Hierbij is de duur van de arbeidsrelatie vaak relatief kort en wordt dus ook regelmatig van baan gewisseld. In de regel worden deze flexibele arbeidskrachten via intermediairs bij bedrijven geplaatst. De contracten verlopen in dat geval via de intermediair, die op papier de werknemer in dienst neemt en detacheert bij een bedrijf. Het gevolg hiervan is dat bedrijven wel steeds om een screening vragen, waarbij dezelfde gegevens vaak geverifieerd dienen te worden. Denk bijvoorbeeld aan een interim werknemer die via Yacht achtereenvolgens bij verschillende banken te werk wordt gesteld. Iedere bank vraagt bijvoorbeeld om een verificatie van het diploma, hetgeen betekent dat meerdere malen hetzelfde diploma gecheckt moet worden bij DUO. Dat is niet alleen omslachtig, maar kost ook iedere keer geld, terwijl het diploma al een keer gecheckt is. Tot op heden worden data echter niet opgeslagen met als doel het nogmaals te gebruiken.

De verwerking van persoonsgegevens door CV-OK is eind 2013 getoetst, en goed bevonden, door het College bescherming persoonsgegevens (CBP). Naast de goedkeuring op het proces en de data verwerking heeft CVOK een separaat verwerkingsbesluit ontvangen om ook strafrechtelijke gegevens te mogen verwerken. De verwerking van persoonsgegevens door CV-OK is bij het CBP geadministreerd onder het meldingsnummer m1417641. De werkwijze van CV-OK is conform de richtlijnen en adviezen van Nederlandse Bank NV, de Autoriteit Financiële markten en de Nederlandse vereniging van Banken, en sluit aan bij de actuele wet- en regelgeving hieromtrent. De focus op financiële instellingen komt vanwege het feit dat in die sector met name wettelijk verplichte screenings plaatsvinden.

CV-OK is ISO-9001 gecertificeerd. Dit is een (internationale) norm voor kwaliteitsmanagement systemen (KMS). Hiermee laat CV-OK zien dat CV-OK de bedrijfsprocessen aantoonbaar beheerst. Uiteraard geldt, ondanks alle certificeringen en besluiten, dat er wel altijd zorgvuldig gewerkt moet worden en dat voldoende waarborgen ingebouwd moeten worden. Kandidaten dienen te allen tijde duidelijk geïnformeerd te worden over de gegevensverwerkingen en de doelen van de verwerking.

De praktijk van arbeidsverbanden van korte duur, die nog extra vaak voorkomt als gevolg van de economische crisis, gaf aan dat er behoefte was aan een alternatieve opzet van het systeem. CV-OK heeft vervolgens YOPS ontwikkeld, waarin de situatie in feite is omgekeerd. De kandidaat beheert een eigen digitale kluis met de gegevens uit voorgaande screenings. De gegevens worden zo bewaard en kunnen dus hergebruikt worden bij een volgende werkgever. De kandidaat betaalt een kleine vergoeding voor het hosten en bijhouden van de kluis, waarin ook de werkervaring geüpdatet kan worden. In het geval van een nieuwe sollicitatie kan de kandidaat een elektronische sleutel aan

de beoogde werkgever verschaffen, waarmee deze toegang krijgt tot de kluis en de voor de opdrachtgever relevante screening kan worden getoond.

3.1.2 YOPS: Your online profile safe

Bij de innovatieve praktijk van Your Online Profile Safe (YOPS) is het systeem omgedraaid ten opzichte van CV-OK. Niet de (potentiële) werkgever is klant, maar de ZZP-er[3] is klant. Deze krijgt de beschikking over een digitale kluis met zijn CV. Het is een digitale omgeving, waarin een ZZP-er zijn werkprofiel kan opbouwen, bijhouden, laten valideren, en delen met (potentiële) nieuwe werkgevers en opdrachtgevers. In het werkprofiel kunnen relevante bestanden worden bijgehouden, zoals CV, ID, VAR, VOG, referenten, etc.

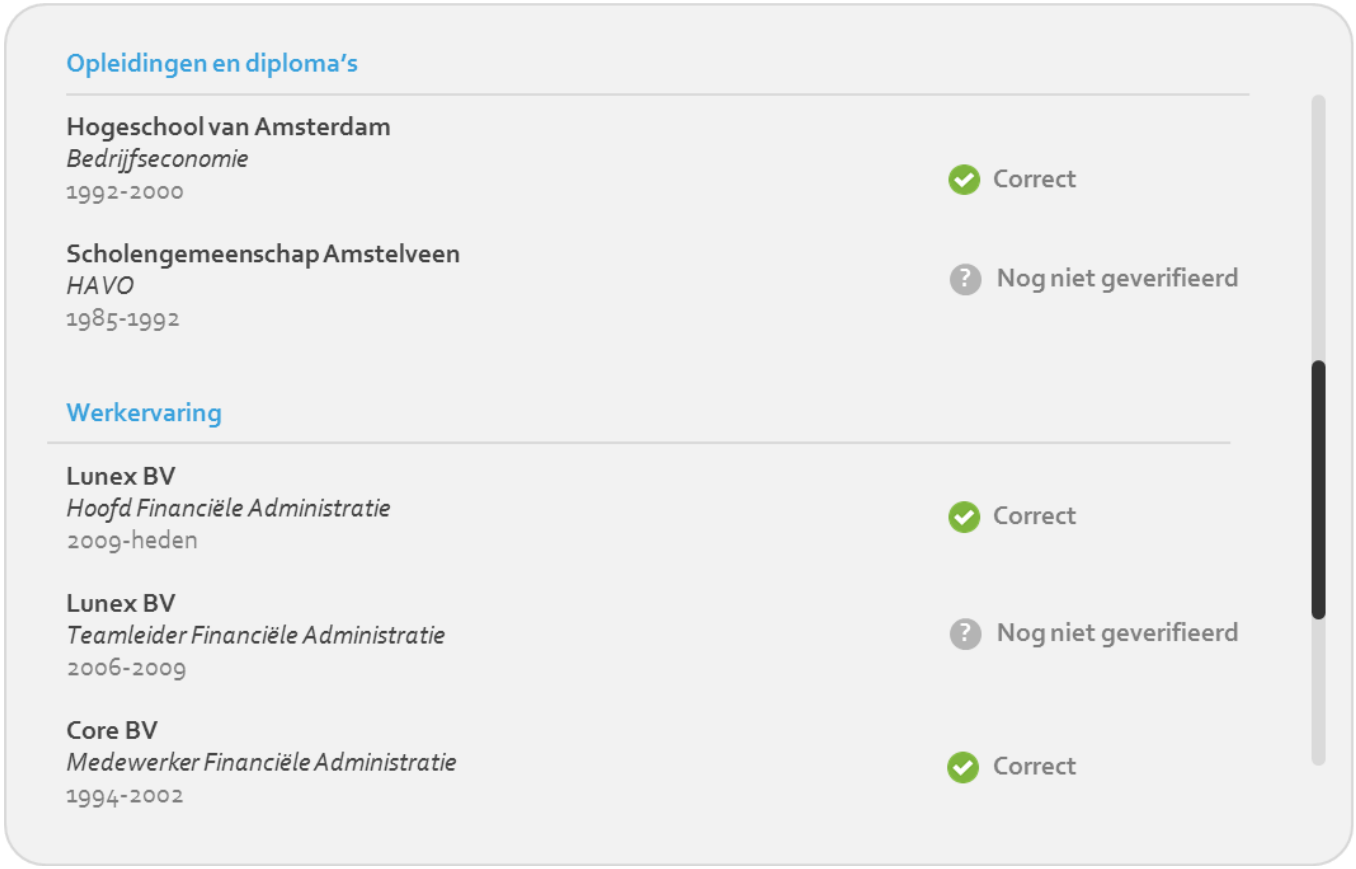
YOPS is dus een systeem om mensen een beveiligde omgeving te bieden waarbinnen hun gegevens gevalideerd zijn en kunnen worden bijgehouden. Updates worden verwerkt en geverifieerd. Het gevolg is dat zodra er een verzoek is van een opdrachtgever voor een screening, deze sneller uitgevoerd kan worden tegen lagere kosten. De controle over het delen van de gegevens in het profiel ligt bij het individu. Hij heeft de keuze om een sleutel te delen met een potentiële werkgever, die daarmee toegang kan krijgen tot de relevante, gevalideerde data binnen zijn profiel. Omdat het individu zelf het profiel beheert kunnen gegevens bewaard blijven en hergebruikt worden voor verschillende werkgevers. Het steeds opnieuw uitvoeren van een volledige screening is niet nodig, omdat alleen eventuele ontbrekende gegevens toegevoegd hoeven te worden. Dat levert een voordeel op ten opzichte van de huidige praktijk, omdat bijvoorbeeld een nog geldige VOG hergebruikt kan worden bij een nieuwe uitzendbaan.

De flexwerker maakt éénmalig een profiel aan met gegevens omtrent opleiding, loopbaan, etc. Via een kijkfunctie kunnen werkgevers een preview van het profiel bekijken. Wanneer een opdrachtgever en flexwerker mogelijk met elkaar verder willen vraagt de opdrachtgever aan de flexwerker om een digitale sleutel in combinatie met het gewenste screeningsprofiel. De flexwerker kan vervolgens snel zijn digitale rapport ter beschikking stellen aan de opdrachtgever. De software van YOPS controleert welke onderdelen al gevalideerd staan in het profiel en voert de screenings onderdelen uit die nog missen. Binnen drie werkdagen levert YOPS het resultaat van de pre-employment screening. Alle resultaten van de screening worden in het profiel opgeslagen en bewaard, zodat deze later, indien nodig, nogmaals gebruikt kunnen worden.

De nieuwe insteek waar bij YOPS voor gekozen is vereiste dat een compleet nieuw systeem gebouwd werd om de diensten aan te kunnen bieden. Er zijn de nodige overlappingen met CV-OK, maar toch is gekozen voor een nieuwe start ‘from scratch’. In het systeem is een Privacy-by-Design benadering gekozen. Gegevens worden automatisch goed beveiligd, zijn alleen met de digitale sleutel toegankelijk, en er wordt niet meer verwerkt dan strikt noodzakelijk of dan de flexwerker zelf aangeeft. Een bepaalde flexibiliteit in het systeem is ook nodig. Gegevens van screenings kunnen bewaard worden, maar de flexwerker kan ook kiezen voor verwijdering van de gegevens. Daarnaast kan het voorkomen dat gegevens slechts voor een bepaalde termijn bewaard mogen worden. Een VAR-verklaring is bijvoorbeeld slechts een jaar geldig en dient dan vernieuwd te worden. Na

[3] Naast ZZP-ers kan YOPS goed gebruikt worden door uitzendkrachten, consultants, etc. Het nut bewijst zich voor arbeidskrachten die flexibel werken en daardoor dus vaak meerdere werkgevers en opdrachtgevers bedienen.

verlopen van de geldigheidsduur is er dus geen sprake meer van een geverifieerde VAR-verklaring. De gegevens kunnen dan verwijderd worden. De historische aanwezigheid van een VAR-Verklaring kan dan overigens wel afgeleid worden uit het werkverleden.



Figuur 1: Een voorbeeld van een overzichtsrapport met deels geverifieerde gegevens.

3.1.3 Conclusie

YOPS is een privacy-innovatie, omdat het systeem expliciet is ingericht om controle bij de gebruiker (het individu) te leggen. Het mooie aan dit voorbeeld is dat het businessmodel en de functionaliteit daar perfect op aansluiten. Een flexwerker heeft er zelf belang bij om zijn CV up-to-date te houden en is naar verwachting bereid daar een kleine vergoeding voor te betalen. Een screeningsrapport is immers nodig om ergens aan de slag te kunnen, dus er staan ook inkomsten tegenover. De toegevoegde waarde zit in de verificatie van gegevens, waarmee de flexwerker zichzelf aantrekkelijker maakt voor potentiële opdrachtgevers, omdat de screening sneller en eenvoudiger uitgevoerd kan worden.

Een goede infrastructuur voor het opzetten van de dienst was niet voorhanden. Deze is daarom 'from scratch' ontwikkeld en is ook anders dan de CV-OK opzet. De gewenste functionaliteiten waren voor YOPS goed te formuleren en zijn vervolgens speciaal ontwikkeld door een softwarebedrijf waarmee al langer werd samengewerkt. Dit bedrijf verzorgt ook alle updates. Juiste kennis voor het opzetten van de dienst was daarom relatief eenvoudig te vinden. De reeds bestaande samenwerking heeft daar vermoedelijk positief aan bijgedragen.

Binnen de infrastructuur wordt gebruik gemaakt van diverse beveiligingstechnologieën. Het online platform van CV-OK is een secure https omgeving, gehost door Mendix (www.mendix.com). Dit is

een snelgroeiend Nederlands bedrijf, dat ongeveer 9 jaar oud is. Mendix beschikt sinds begin dit jaar over een ISAE 3402 verklaring (http://www.isae3402.nl/) , wat de SAS70 standaard vervangt en een niveau van cloud beveiliging en beheersing van financiële- en ICT processen aangeeft. CV-OK en YOPS mogen, als afnemer van die cloud, een 'beroep' doen op de ISAE 3402. Vanaf het begin van de samenwerking met Mendix staan de data bij XS4all in NL, en dat mag ook niet naar een buitenlandse server zonder toestemming van CV-OK / YOPS. Zodoende is geborgd dat zij, voor zover mogelijk, onder de voor hen relevante jurisdictie blijven vallen (en dus niet indirect onder de VS).

3.2 NS

3.2.1 Privacy in de organisatie

NS is bewust bezig met de inbedding van privacy in de organisatie en bij de ontwikkeling van nieuwe diensten en de optimalisering van bestaande diensten. Hierbij is een centrale rol belegd bij de Privacy Officer (PO). De PO ziet toe op privacy inbedding in ontwikkeltrajecten, maar maakt het onderwerp privacy ook toegankelijk voor alle lagen binnen de organisatie door middel van een open cultuur waarbij de deur van de PO altijd openstaat voor collega's, maar ook meer geformaliseerd door het houden van een maandelijks spreekuur. De PO kan daadwerkelijk en effectief toezicht uitoefenen door vergaande interventiebevoegdheden, waaronder de zogenaamde 'kill switch'; de mogelijkheid van de PO om een project (tijdelijk) stil te leggen totdat privacybezwaren zijn weggenomen. Voorbeelden van de ontwikkeling van diensten waarbij privacy een belangrijk design criterium is zijn de optimalisering van looproutes op de perrons, de verdeling van reizigers over coupés en de Schiphol Garantie Service. In onderstaande worden alle drie deze pilot projecten kort besproken.

3.2.2 SMART Station

Onder de noemer 'SMART Station' is een volgsysteem voor stations ontwikkeld om de dienstverlening op het station beter af te stemmen op de behoefte van reizigers maar ook om de commerciële mogelijkheden die een station biedt optimaal te benutten.[4] Smart Station is uitgerold op station Groningen en Utrecht CS. Onderzoek heeft uitgewezen dat het slim inrichten van de looproutes van reizigers het bestedingspatroon van de reiziger op het station positief kan beïnvloeden. Ook de intensiteit van het gebruik van de looproutes is een belangrijk aspect om de exploitatie van het station te verbeteren. *"Inzicht in aantallen, looptijden en wachttijden is belangrijk voor de inrichting van transfervoorzieningen zoals roltrappen, trappen, deuren, perrons en passages."*[5] Om de meest optimale looproutes in kaart te brengen is het noodzakelijk stromen van reizigers te analyseren. Om dit te laten doen door menselijke telling is erg duur, terwijl vrij eenvoudig en goedkoop hiertoe technologie ingezet kan worden. NS stond dan ook voor de vraag met welke methode op geautomatiseerde wijze passantenstromen op stations over een langere periode inzichtelijk gemaakt konden worden. Door de specifieke kenmerken van passantenstromen op stations, ineens heel veel passanten tegelijk, en allemaal komend en gaand in verschillende richtingen, bleken bestaande voorhanden zijnde technologieën – zoals Bluetoothmetingen voor

[4] De informatie over het slimme station is gebaseerd op een beleidsdocument van de NS getiteld: Information Policy Plan SMART Station Version 2.0. en op een artikel van Jeroen van den Heuvel, Eelco Thiellier en Niels van Gerwen: Privacy by Design bij reizigers metingen op Stations, Privacy & Compliance, 2013-3, p. 17-21.

[5] Van den Heuvel et al. 2013, p. 17.

auto's – niet geschikt. Daarom is samen met NPC[6] een nieuw passantvolgsysteem ontwikkeld waarvan het doel als volgt is omschreven: *"gain insight at the system level into (1) the pedestrian flows, walking routes, waiting times and waiting locations of passengers and visitors to railway stations and in the areas around the railway stations and (2) the actual travel times of passengers in the network of railway stations.*

"SMART Station bestaat uit drie modules: 1. tel- en volgmodules op basis van infraroodtechnologie; 2. analysemodule; 3. presentatiemodule. Het volgen van reizigers gebeurt door op verschillende plaatsen in een station de MAC-adressen (unieke hardwarenummers) van Bluetooth- en WiFi-apparaten op te vangen. Door de sensoren strategisch te plaatsen, kan aan de hand van de MAC-adressen, detectietijdstippen en de plaats van sensoren een reconstructie worden gemaakt van de looproute van een reiziger. Ook wordt bepaald hoe lang de reiziger over deze route heeft gedaan. De gegevens van de volgsensoren worden door de analysemodule gecombineerd met de gegevens uit de telsensoren (dit aangezien een persoon geen mobiel apparaat bij zich kan dragen of Bleutooth en/of WiFi uitgeschakeld kan hebben). De presentatiemodule kan op elk gewenst moment een totaalbeeld van de reizigersstroom op een station weergeven.

Privacy is gewaarborgd doordat het niet mogelijk is een MAC-adres te linken aan gegevens over de eigenaar/gebruiker van de apparatuur. Er worden enkel nummers weergegeven om op anonieme wijze de verschillende reizigers te kunnen onderscheiden. Gebruikers van SMART Station kunnen die nummers niet gebruiken voor identificatie.

Ook is er een 'informatiebeleidsplan' voor SMART Station waarin beschreven is op welke wijze privacy gewaarborgd wordt in de technologie, processen en organisatie van SMART Station. In de technologie kan gewezen worden op onomkeerbare versleuteling van de door de telmodule ingewonnen MAC-adres gegevens ('one way-hashing'). Dit maakt het mogelijk de originele gegevens direct bij de bron te vernietigen. De versleuteling wordt gecombineerd met datum-informatie, waardoor de hash van hetzelfde MAC-adres elke dag een andere telcode oplevert en er dus geen profielen van terugkerende reizigers opgebouwd kunnen worden. Op het niveau van het proces kan erop gewezen worden dat na analyse de gegevens automatisch weggegooid worden en dat er gewerkt wordt met verschillende autorisatieniveaus waardoor slechts een beperkte groep personen toegang tot de gegevens heeft. Ook in het inkoopproces is privacy een criterium: leveranciers moeten aantonen dat ze volledig volgens het informatiebeleidsplan SMART Station werken. Op het niveau van de organisatie wordt privacy ingebed door medewerkers te informeren over het informatiebeleidsplan. Ook wordt iedere twee jaar getoetst of het informatiebeleidsplan SMART Station nageleefd wordt. Ook hier geldt de 'kill switch' bevoegdheid van de PO om bij gerede twijfel over zorgvuldig handelen door NS, NPC en/of de leveranciers het systeem uit te schakelen totdat knelpunten zijn opgelost.

3.2.3 Pilot IJssellijn

Ook bij de ontwikkeling van een andere dienst wordt gebruik gemaakt van reizigers tellingen. Het gaat om het beschikbaar stellen van een app waarop de reizigers kunnen zien wat de actuele reizigersaantallen in de trein zijn op basis waarvan de reiziger zelf keuzes kan maken zoals wel/niet en waar in de trein instappen, alsmede opties voor andere keuzes, zoals een ander traject en/of een

[6] NPC is het projectmanagement- en adviesbureau voor NS, ProRail en regionale vervoerders voor (her)ontwikkeling van stationsgebieden. Van den Heuvel et a. 2013, p. 17.

ander tijdstip. De pilot heeft plaatsgevonden op de IJssellijn (Zwolle-Roosendaal) waar middels infraroodsensoren de actuele reizigersaantallen werden vastgesteld: *"Een deel van het rijdend materieel op het proeftraject is voorzien van sensoren die exact het aantal reizigers tellen dat de sensor passeert. De actuele reizigersaantallen worden draadloos ontsloten naar de wal en verzameld in een database. Deze actuele reizigersaantallen, gecombineerd met reisinformatie, voeden de app".*[7]

Naast de hoofddoelstelling kent de proef nog een aantal bijkomende doelstellingen zoals het verstrekken van de actuele reizigersaantallen aan de eerstelijns medewerkers zodat zij beter reisadvies aan klanten kunnen verstrekken; het ondersteunen van de bijsturingsorganisatie in verstoorde situaties in het managen van het materieel, personeel, de dienstregeling en in de dienstverlening; het toetsen van de ketenbetrouwbaarheid van de informatie om deze op termijn inzetbaar te maken bij de operatie (planning personeel en materieel); het toetsen van de '(be)stuurbaarheid' (beïnvloeden van gedrag) van de klant, waardoor andere toepassingen commercieel interessant kunnen worden.

3.2.4 Schiphol Garantie Service[8]

De Schiphol Garantie Service (SGS) is een dienst van NS, in nauwe samenwerking met Schiphol, waarbij reizigers gegarandeerd wordt tijdig op Schiphol aan te komen om een vlucht te halen. In 2014 wordt deze dienst als pilot voor de eerste maal aangeboden van 14 juli tot en met 1 september. De kosten voor deze dienst bedragen, tenminste in de pilotfase, voor de consument 5 euro per keer. De dienst werkt via een reizigers app die na betaling kan worden gedownload. De app, die zowel voor Iphone en Android-telefoons ontwikkeld is, maakt het mogelijk de treinreis van klanten (die zich van te voren aanmelden) te volgen. Vooraf geeft de reiziger vertrekstation, datum/vertrektijd vlucht, vluchtnummer, aantal personen en koffers op. Deze gegevens vormen de input voor een reisadvies op maat aan de reiziger. Die gegevens worden ook opgeslagen en gebruikt door NS om de reis te monitoren op onvoorziene omstandigheden. De SGS-reisplanner biedt de klant notificaties, via sms of telefoon, mocht er onverhoopt iets verkeerd gaan en geeft dan een nieuw reisadvies. Indien een situatie ontstaat waarin de trein mogelijk Schiphol niet tijdig bereikt, wordt door NS een taxi of een bus geregeld. Ook staat er op Schiphol iemand gereed om de reiziger te begeleiden naar de incheckbalie. Mocht de vlucht onverhoopt niet gehaald worden, dan betaalt NS de kosten van een nieuw vliegticket of de kosten van een omboeking en mogelijk zelfs de kosten voor een eventuele overnachting in een hotel.

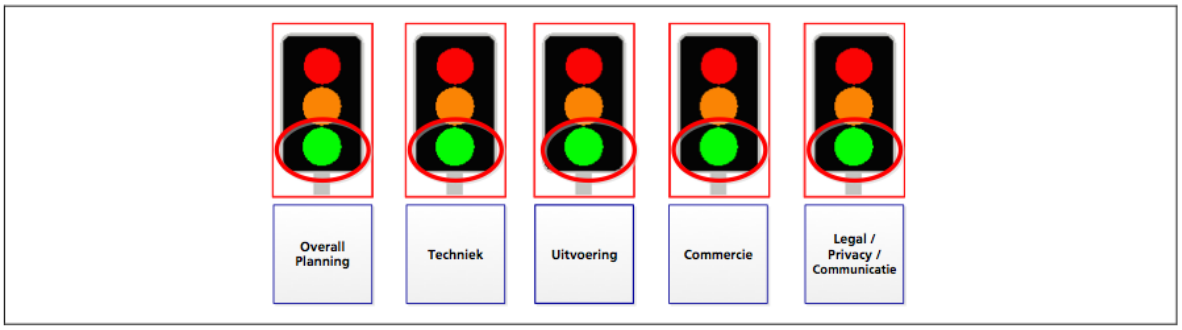
De dienst is bedoeld om de reiziger te ontzorgen en meer comfort te bieden in het geval zij op (zaken)reis gaan met trein en vliegtuig. De pilot past in een breed pakket aan maatregelen om de bereikbaarheid van Schiphol per OV, en het vertrouwen daarin, te vergroten. Op basis van een grondige evaluatie besluit NS of de service eventueel structureel kan worden ingevoerd.

Interessant aan deze Service is dat deze is binnengekomen via het maandelijkse spreekuur van de Privacy Officer van NS. De bedenker van de Service is, alvorens met de uitwerking van zijn idee te starten, advies gaan vragen bij de PO, waardoor privacy van meet af aan is meegenomen in het

[7] Presentatie Jantina Woudstra Programma manager NS, beschikbaar gesteld door Privacy Officer NS (Rachel Marbus).

[8] Informatie over de Schiphol garantie service beschikbaar via http://nos.nl/artikel/665220-ns-verzekert-aankomst-op-schiphol.html en http://www.ns.nl/over-ns/nieuwscentrum/nieuwsberichten/2014/06/proef-met-schiphol-garantie-service-van-start.html

ontwikkelproces. Dit heeft ertoe geleid dat de keuze is gemaakt zo min mogelijk informatie te verzamelen. Hoewel tijdens het ontwikkeltraject allerlei leuke features werden bedacht, zoals bijvoorbeeld het door de reiziger aanmaken van een profiel met foto, is geredeneerd vanuit het privacy concept data minimalisatie, en is besloten alleen die gegevens te verwerken die daadwerkelijk noodzakelijk zijn voor het aanbieden van de SGS dienst. Zo worden bijvoorbeeld alleen de gegevens verwerkt van degene die de SGS koopt. Ook al reist hij met een gezelschap van tien personen, en wordt van al deze personen bagage opgegeven, worden geen gegevens van deze medereizigers verwerkt. Het belang van privacy is ook duidelijk zichtbaar in de interne communicatie rondom dit traject, waarbij met behulp van stoplichten inzichtelijk is gemaakt hoe het er binnen bepaalde domeinen - relevant voor de ontwikkeling van de SGS - voorstaat. Privacy is hier uitdrukkelijk in benoemd. Zie figuur 2.



Figuur 2: Stoplichten betreffende interne communicatie.

3.2.5 Conclusie

Bij NS is een constant proces gaande van het ontwikkelen van nieuwe diensten en het optimaliseren van bestaande diensten. Privacy vormt hierbij een belangrijke beleidsoverweging. Door de centrale rol van de Privacy Officer, de inbedding van privacy in alle lagen van de organisatie, en het daadwerkelijk beleggen van ver strekkende bevoegdheden bij de Privacy Officer, is sprake van privacy innovatie binnen de gehele organisatie. Bewustwording op de werkvloer wordt ondersteund door een privacy spreekuur met de Privacy Officer, de bevoegdheid daadwerkelijk in te grijpen is gewaarborgd door de zogenaamde 'kill switch' en bij de ontwikkeling van nieuwe diensten – optimalisering passantenstromen, verdeling reizigers over de trein en de Schiphol Garantie Service – wordt privacy van meet af aan meegenomen als kerncriterium in het ontwikkelproces. Dat privacy niet alleen een kerncriterium, maar ook een driver kan zijn in innovatietrajecten wordt onderkend door Van den Heuvel et al.: *"De ontwikkelingen in techniek gaan immers razendsnel. Dit biedt kansen om reizigersmetingen steeds sneller, slimmer en goedkoper uit te voeren. Privacy helpt niet alleen om alert te blijven op risico's en knelpunten, maar blijkt ook een driver voor innovatie."*[9]

[9] Van den Heuvel et al., p. 21.

4 Externe factoren: het juridisch kader

Een belangrijke factor in het kader van privacy en innovatie is vanzelfsprekend het juridisch kader. Met name de Wet bescherming persoonsgegevens (Wbp) en in bepaalde gevallen ook de Telecommunicatiewet (Tw) stellen tal van eisen aan digitale dienstverlening. Bovendien is dit kader volop in beweging, aangezien er op Europees niveau een Algemene Verordening Gegevensbescherming aankomt die de nodige aanpassingen op de huidige Wbp met zich mee zal brengen. Over het algemeen lijkt ingezet te worden op strengere eisen en uitgebreidere bevoegdheden voor toezichthouders. Daarnaast is een aantal concepten, zoals Privacy/Data Protection by Design en het recht om vergeten te worden nadrukkelijk aanwezig.

Het juridisch kader is een gegeven van buitenaf waar bedrijven mee om moeten gaan. Op welke wijze ze dat doen en wat de juridische eisen betekenen voor innovatie in de praktijk verschilt van geval tot geval. Om een beter beeld te krijgen van de invloed van regelgeving op privacyvriendelijke innovatie en welke aspecten in de praktijk worden ervaren is in het kader van dit Actieplan een expert-workshop georganiseerd. De belangrijkste punten die in de workshop door de deelnemers naar voren zijn gebracht zijn, worden in dit hoofdstuk besproken. Een uitgebreid verslag van de workshop, evenals de inleidende pitches, zijn als Annex 1 en 2 bij dit rapport gevoegd.

In de workshop stond de volgende vraag centraal: *"Hoe bij te dragen aan acceptatie en implementatie van privacy-innovaties en welke rol speelt het huidige wettelijke kader hierin, of zou het huidige wettelijke kader hierin moeten spelen?"* De respons op deze vraag wordt hier behandeld langs de lijnen van innovaties, bedrijven/praktijk, burgers/consumenten, en overheid. De weergaven hieronder zijn dus gebaseerd op de inbreng van de deelnemers in de workshop.

4.1 Innovaties

De invloed van regelgeving op het vlak van innovatie heeft twee belangrijke componenten. Ten eerste is er de regelgeving zelf die rechtstreeks uitdaagt tot innovatie. Zowel voor bedrijven als voor consumenten kunnen grote voordelen behaald worden bij het stevig doorzetten van privacy-innovaties. Dat vertaalt zich in de praktijk in anticipatie op de aankomende Verordening. Het organiseren van Privacy by Design en Data Protection by Design vereist van organisaties dat zowel technisch als organisatorisch wordt ingegrepen. Beide aspecten kunnen innovaties bevatten. De technische aanpak omvat bijvoorbeeld het ontwikkelen en inzetten van design patterns voor data processing, data transfer, data management etc.; het inzetten van privacybeschermende technologieën dus om op die wijze te voldoen aan de regelgeving.

Organisatorische innovatie op het vlak van de bedrijfsvoering is mogelijk door het structureel inbedden van privacy in de organisatie. Het aanstellen van een privacy officer is een goed startpunt. Innovatiever is het inzetten van bijvoorbeeld privacy champions op de werkvloer. Deze zorgen voor draagkracht voor en naleving van privacy in de gehele organisatie en voor een geïnstitutionaliseerde aanwezigheid van privacy in alle lagen van de organisatie.

De tweede component waar regelgeving innovatie kan beïnvloeden is regelgeving als meetinstrument. Compliance is een minimum vereiste. Waar mogelijk kan dus getracht worden om proactief verdere stappen te zetten en om diensten privacyvriendelijk in te richten. Op dat moment wordt privacy ingezet als marktdifferentiator en profileren organisaties zich als privacyvriendelijk.

Het regelgevend kader is dan dus de nullijn waar organisaties bovenuit willen steken. Het creëren en versterken van vertrouwen speelt in dit geval een belangrijke rol. In de workshop werd aangegeven dat PIA's en transparantierapporten vaak niet door consumenten gelezen worden, maar wel kunnen dienen als instrument om vertrouwen op te wekken wanneer deze openbaar worden gemaakt. Tevens werd opgemerkt dat goede communicatie vanuit bedrijven essentieel is. Een organisatie moet helder aan de consumenten kunnen uitleggen welke stappen gezet worden en waarom, en vooral wat dat voor de consument betekent.

4.2 Bedrijven/praktijk

Voor bedrijven ligt de uitdaging in het vinden van een business model waarbinnen privacyvriendelijk geopereerd kan worden. Een eerste stap is bewustwording over de noodzaak van compliance. De hogere boetebevoegdheden zoals voorgesteld in de Verordening zullen daaraan bijdragen. De regelgeving zal op dit punt dus een zekere stimulerende werking hebben. Het betreft dan een negatieve prikkel in de vorm van handhaving en sancties. Tegenover de stimulerende werking wordt in de workshop echter gesteld dat daarmee ook juist de uitstraling van privacy als kans opzij geschoven wordt, omdat privacy nog sterker als bedrijfsrisico wordt neergezet. Dat kan een bedrijfseconomische afweging in de hand werken.

In het kader van een business model wordt ook gedacht aan privacy als unique selling point. Compliance wordt daarmee omgezet naar een positioneringsinstrument. Dit biedt tot op zekere hoogte kansen. Kritiek van de experts op dit punt richt zich echter op de beperkingen van deze benadering. Compliance is immers voor iedereen een wettelijke verplichting en kan daarom op zichzelf niet als unieke benadering gelden. Dat is pas het geval wanneer er verder gekeken wordt dan compliance en wanneer privacy dus integraal in de bedrijfsvoering en in producten en diensten wordt meegenomen.

4.3 Burgers/Consumenten

In de workshop wordt aangegeven dat de verantwoordelijkheid voor privacy en gegevensbescherming niet volledig bij de consument gelegd kan worden. Consumenten zijn zich, volgens de experts, te weinig bewust van wat er allemaal speelt en hebben onvoldoende expertise om zich hiertegen met technische oplossingen te wapenen. Het blijkt echter lastig aan te geven wat precies wel en niet van de consument verwacht mag worden. Met name burgerrechtenorganisaties geven aan dat er een tendens gaande is waarbij steeds meer van de consument verwacht wordt, terwijl er een toenemende asymmetrie is tussen bedrijven en consumenten voor wat betreft kennis en informatie over het verwerken van gegevens.

4.4 Overheid

De overheid heeft een vanzelfsprekende rol als regelgever. In die rol speelt altijd de uitdaging om tijdig in te springen op technologische ontwikkelingen en tegelijkertijd de regelgeving neutraal genoeg op te stellen om geen lacunes te creëren. Volgens de experts staat de overheid positief tegenover zelfreguleringsinitiatieven, waarmee een deel van dit probleem wordt opgelost. Wetgeving wordt in die gevallen gezien als een *ultimum remedium* wanneer zelfregulering onvoldoende bijdraagt aan de opname van privacyinnovaties in de praktijk. De experts geven echter ook aan dat pure zelfregulering, zonder sturing vanuit de overheid vaak niet de beoogde bescherming van consumenten oplevert.

De overheid kan zich ook actief opstellen in de ondersteuning bij de naleving van regelgeving. Ze kan bijvoorbeeld intermediairs proberen aan te sturen. Belangenorganisaties, zoals bijvoorbeeld de Consumentenbond, kunnen een rol spelen in het vergroten van het online vertrouwen van consumenten en in het zorgvuldig gebruik van data door dienstverleners.

In het verlengde van de overheid zien de experts nog kansen voor ondersteuning door de toezichthouder. Niet voldoen aan privacyvereisten is bij bedrijven lang niet altijd een zaak van onwil, maar vaak een zaak van onwetendheid en onkunde. Bedrijven weten ook niet wat ze moeten doen aan beveiliging. Experts signaleren daarom een behoefte aan een set minimale voorwaarden waaraan voldaan moet worden en waarop het CBP niet alleen handhaaft, maar ook voorlichting geeft. Dit kan voor bedrijven ook kostenverlagend werken. De invulling van de rol van de toezichthouder wordt niet als onderdeel van dit rapport ter discussie gesteld. Enige voorlichting en praktische voorbeelden kunnen echter snel voordeel opleveren en het algehele niveau van privacybescherming verhogen. Naast de toezichthouder kan een dergelijke voorlichtingstaak wellicht ook door brancheorganisaties of andere organen opgepakt worden. Voorop staat wel dat adviezen via de huidige kanalen van het CBP en de Artikel 29 Werkgroep zeker voor niet-juristen moeilijk te behappen zijn.

4.5 Tussenconclusie

Uit de workshop kwamen drie oorzaken naar voren die enige beweging op het gebied van privacytechnologie verklaren:

1. De markt wordt volwassen
2. Privacy wordt gezien als differentiator
3. Anticipatie op verordening

De experts gaven ook aan dat het huidige wettelijke kader te ingewikkeld is voor burgers en bedrijven. De verantwoordelijkheid voor bescherming van privacy en gegevensbescherming door gebruik te maken van privacy-innovaties kan niet bij de burger gelegd worden. Zelfs met een toenemend bewustzijn onder burgers is er onvoldoende zicht op de risico's en zijn burgers onvoldoende kundig om (technische) innovatieve maatregelen te implementeren en kunnen ze de markt niet significant beïnvloeden.

Er blijft een inherent spanningsveld om oplossingen in de wetgeving te zoeken. Immers, als het huidige reguleringskader, waar veel reeds in is opgenomen, niet werkt, waarom zou een nog uitgebreider kader dan wel werken? Bij bedrijven zal er alleen sprake zijn van uptake als er positieve dan wel negatieve prikkels geboden worden die het bedrijfsbelang van implementatie van dataprotectiemaatregelen duidelijk maken. Hier kan wetgeving wel een rol in spelen aangezien de wet positieve en negatieve prikkels kan genereren: controle en handhaving, hogere boetes, keurmerken, subsidies, etc. Hoewel bedrijven privacy steeds meer als markt zien, moet hierbij worden opgemerkt dat wat gepretendeerd wordt met betrekking tot privacy, lang niet altijd een correcte weergave van de werkelijkheid is. Burgerrechtenorganisaties noemen voorbeelden waar gepoogd wordt privacy als *selling point* te benutten, gebruik makend van de onwetendheid van de burger over de daadwerkelijke invulling van de privacy standaard. Vanuit dit perspectief kan geopperd worden dat de adoptie van privacy-innovaties niet aan bedrijven kan worden overgelaten.

Aan de andere kant wordt door enkele experts beargumenteerd dat juist door de toename in negatieve prikkels (meer controle, meer audits, meer verantwoording op bijvoorbeeld jaarrekeningen, hogere boetes) en de positieve prikkels die hiermee samenhangen in de zin van kostenbesparing, efficiëntie en privacy als *selling point*, we gewoon nog even geduld moeten hebben omdat de markt het wel degelijk op zal pakken: ze moeten wel, omdat het huidige en toekomstige juridische kader dit afdwingt.

Meer positief noemen de experts keurmerken als een stimulans voor de uptake van privacy innovaties. Simpele inzichtelijke online tools, zoals bijvoorbeeld ☺ en ☹ zijn begrijpelijk voor burgers en vormen een middel voor bedrijven om zich te profileren. Hierbij geldt dan wel dat een toezichthoudend orgaan, een belangen- of brancheverenigingen (partijen als het CBP, Consumentenbond) toezicht en controle uit moeten oefenen en het ontnemen van het keurmerk en eventueel andere sancties tot de mogelijkheden moeten behoren. Een andere mogelijke prikkel is gelegen in zogenaamde Transparency Reports, een in de VS bekend fenomeen. Het zijn vergelijkende rapporten (de Amerikaanse burgerbeweging Electronic Frontier Foundation geeft ratings aan bedrijven over hoe ze omgaan met gegevens). Uit de discussie volgt dat het regulerend kader niet alleen hekken moet zetten, maar juist ook moet stimuleren.

Bij het aanbieden en ontwikkelen van privacy-innovaties geven de experts aan dat sommige wettelijke concepten in de praktijk niet werken, zoals bijvoorbeeld geïnformeerde toestemming, dat als veel te breed en onoverzichtelijk wordt ervaren. Een dergelijk vereiste zal dan ook op een wijze vormgegeven moeten worden waarin het doel van de wet mogelijk wel tot zijn recht komt, zoals bijvoorbeeld het aanbieden van vormen van layered consent. Ook gebruikersvriendelijkheid, voorlichting en assistentie zijn belangrijke voorwaarden om privacy-innovaties bij burgers te laten landen. Burgers hebben online vertrouwen nodig. De achterliggende vraag is dus of het de privacy zelf is die innovatie belemmert, of dat het ontbreken van vertrouwen innovatie belemmert?

5 De directe omgeving: branches en de rol van brancheorganisaties

Brancheorganisaties kunnen een belangrijke rol spelen in het stimuleren van privacy-innovatie. Als organisatie met veel leden hebben zij immers een groot bereik en een goed beeld van de wensen en vragen binnen de branche die zij vertegenwoordigen. Als organisatie kunnen zij dus een coördinerende functie oppakken om gezamenlijk vragen aan te pakken, maar ook een informatieportaal vormen richting alle leden. De directe omgeving van bedrijven speelt dus ook een rol in privacy als innovatie.

5.1 De bijdrage in de huidige praktijk

Privacy-innovatie hoeft niet per se om nieuwe uitvindingen of technologieën te gaan. Ook het stimuleren van privacybescherming door betere naleving van wet- en regelgeving valt hieronder. Een mooi voorbeeld hiervan is de vertaalslag die de DDMA heeft gemaakt als brancheorganisatie van de regelgeving voor privacy en direct marketing naar de praktijk van non-profit organisaties. Onder de titel “Wet & werkelijkheid” heeft de DDMA een gratis brochure opgesteld met uitleg van regelgeving in verschillende toepassingen (email, papieren post, telemarketing, cookies) en hoe daaraan voldaan kan worden. De brochure bevat stroomschema’s aan de hand waarvan eenvoudig bekeken kan worden welke vereisten gelden en wat wel en niet wettelijk is toegestaan en onder welke voorwaarden. De inzichtelijkheid maakt het voor non-profit organisaties, die vaak klein van omvang zijn en geen aparte juristen in dienst hebben, makkelijker om compliant te zijn met privacy regelgeving. Vanzelfsprekend heeft dit ook een positieve weerslag op de consument die beter beschermd wordt.

Onder de noemer “Wet & werkelijkheid” heeft de DDMA ook een handleiding cookiewet opgesteld. Deze is ook gratis te downloaden van de DDMA website. Specifiek op dit dossier geeft de DDMA aan dat er duidelijkheid en transparantie noodzakelijk is en dat zij een actieve rol speelt in het debat. *“Gezien de grote onduidelijkheid in de sector hebben wij er ditmaal voor gekozen de handleiding voor iedereen beschikbaar te stellen. Want door actief bij te dragen aan transparantie in dialoogmarketing, kan DDMA maximaal inzetten op gebalanceerde wetgeving. Regels die rekening houden met het economisch belang van het bedrijfsleven en innovatie in ICT, zonder dat zij afbreuk doen aan de consumentenbescherming.”,* aldus Diana Janssen, directeur DDMA.[10] Hier wordt zichtbaar dat de brancheorganisatie invloed wil uitoefenen op wetgeving. Vanzelfsprekend is dit in het belang van de leden. Bijkomend effect is echter dat er in de gehele breedte van een branche een gedeeld beeld ontstaat van wetgeving en hoe deze in de praktijk toegepast dient te worden. Wanneer het over wetgeving op het gebied van privacy gaat, zoals bijvoorbeeld met de cookiewetgeving, betekent dit dus ook dat de gehele branche zich bewust is van de vereisten uit wetgeving en hoe hier mee omgegaan dient te worden. Uiteindelijk heeft dit tot gevolg dat de compliance met privacyregelgeving in een branche wordt verhoogd, wat dus een positief effect heeft op de privacybescherming van betrokkenen.

In bovengenoemde voorbeelden gaat het om de functie van een brancheorganisatie als informatieportaal richting de aangesloten leden. Informatie wordt breed beschikbaar gesteld, soms voor iedereen die geïnteresseerd is, soms alleen voor leden. Als organisatie kan ook namens een

[10] Zie: https://ddma.nl/privacy/ddma-publiceert-handleiding-cookiewet-wet-en-werkelijkheid/.

branche opgetreden worden om belangen te behartigen in wetgevingsprocessen en andere aangelegenheden.

Een andere functie is het optreden als stimulerend orgaan voor privacy-innovatie. Een voorbeeld in deze categorie kan gevonden worden bij Nederland ICT. Deze brancheorganisatie heeft een aparte privacycommissie. Het doel van deze commissie is om actief deel te nemen aan het privacydebat in Nederland. Het uitgangspunt daarbij is dat er een gezonde balans moet zijn tussen ICT, innovatie en privacy. Nederland ICT ziet ICT en privacy als 'bondgenoten' en geeft aan dat ICT privacy kan bevorderen. Veel van de risico's voor privacy komen voort uit ICT toepassingen, zoals sociale netwerksites, internetbankieren en elektronisch winkelen. Ook op het gebied van identificatiemethoden treden soms risico's of onregelmatigheden op. Een actieve houding ten aanzien van privacy in de ontwikkeling en uitrol van nieuwe ICT-gebaseerde diensten is daarom op zijn plaats. De brancheorganisatie is om die reden dan ook voorstander van Privacy by Design.

In het verlengde van het pleidooi voor Privacy by Design geeft Nederland ICT aan dat een proactieve rol van de toezichthouder (het CBP) gewenst is. De taak van het CBP zou daarmee tweeledig zijn: enerzijds een juridische rol waarbij handhavend wordt opgetreden ten aanzien van de naleving van de privacy regelgeving. Anderzijds een rol waarbij innovatie op het gebied van privacy gestimuleerd wordt door gedurende innovatietrajecten de dialoog aan te gaan met bedrijven en ontwikkelaars. Daarmee kan voorkomen worden dat projecten achteraf afgekeurd worden, omdat ze niet (voldoende) aan de Wbp voldoen, en dat er veel geld verloren gaat aan innovatietrajecten die later geen uitvoering vinden of aanpassingen behoeven.

Nederland ICT levert ook regelmatig een bijdrage aan symposia en andere meetings, vaak in een faciliterende of organiserende rol.

VNO-NCW en MKB-Nederland treden op namens het midden- en kleinbedrijf. Ook binnen deze organisatie is er een aparte privacycommissie. Een belangrijke rol ligt in de publieke consultatie van het CBP wanneer de toezichthouder Richtsnoeren wil uitvaardigen. In de consultatie worden dan een aantal vertegenwoordigers, waaronder VNO-NCW en MKB-Nederland, benaderd om feedback te geven. Op dergelijke momenten kijkt de privacycommissie gedetailleerd naar het voorstel en geeft daar feedback op. De Richtsnoeren zijn uiteindelijk immers uitgevaardigd vanuit het perspectief van de toezichthouder en vertegenwoordigen daarmee niet altijd een breed gedragen maatschappelijke visie. De privacycommissie tracht dan een weerklank te geven vanuit de visie van de maatschappij en het bedrijfsleven. Los van de consultaties heeft VNO-NCW regelmatig een informeel onderhoud met vertegenwoordigers van het CBP in een soort benen-op-tafel-sessie om signalen uit te wisselen.

VNO-NCW en MKB-Nederland zijn wel van mening dat meer helderheid vanuit het CBP wenselijk is. Dat wil niet noodzakelijk meteen zeggen dat het CBP aan moet geven wat precies wel en niet mag. Het zou meer gewenst zijn in de vorm van een informele benen-op-tafel-sessie waarbij een bedrijf in gesprek met het CBP op informele wijze een innovatie tegen het licht kan houden. Daarbij kan een denkrichting beschreven worden en om sturing gevraagd worden. Het belangrijkste doel hiervan is het voorkomen dat innovatie teniet wordt gedaan, doordat achteraf een bedrijf door de toezichthouder wordt teruggefloten.

In de opvattingen van VNO-NCW en MKB-Nederland is een regulerend kader als "stick" benadering niet wenselijk: innovatie moet toch uit de markt komen. Dat is des te meer het geval wanneer

privacy wordt benaderd als een unique selling point: dat kan je per definitie niet opleggen. In de praktijk lijkt compliance op zich echter vaak al genoeg inspanning te vergen, zeker voor MKB bedrijven. De verwachting is dat dat met de aankomende Verordening alleen maar sterker wordt.

Certificering van bedrijven die hun diensten privacy-vriendelijk hebben ingericht kan mogelijk wel helpen als positieve prikkel. Daarbij dient echter wel een kanttekening gezet te worden dat het ook een *barrier to enter the market* kan zijn. Partijen die de open norm van de wet invullen op basis van hun eigen invulling (kan ook compliant zijn!) vallen buiten de lijn van certificering. Zij zijn dus mogelijk wel 100% compliant, maar hebben geen geld (over) voor het aanvragen van een certificering. Het niet hebben van het keurmerk leidt dan tot een competitieve achterstand.

Als praktisch hulpmiddel is in juli 2014 de Privacy Quick Scan gelanceerd. In 3 stappen, en totaal 14 vragen geeft het ondernemers een beeld of ze goed bezig zijn voor klant en werknemer en als bedrijf. Het is nadrukkelijk geen check op wettelijke vereisten, maar op de interactie met je klant of werknemer en of je dat goed doet. Ook al is alles wettelijk in orde, dan nog is bijvoorbeeld goede communicatie essentieel. De Privacy Quick Scan geeft dus een beeld van het bedrijfsbelang, maar ook van het belang van de klant. De waarborgen en kaders die je moet inrichten zijn bijvoorbeeld afhankelijk van het type proces of het type gegevens waarmee je werkt (bijv. bij medische gegevens sterkere waarborgen vereist). Het doel van de Privacy Quick Scan is om awareness te kweken bij bedrijven en haakjes te bieden om verder risico's aan te kunnen pakken. Het geeft geen juridisch advies, maar wel een indicatie over hoe goed de werkwijze van een bedrijf is ten aanzien van klanten, werknemers en het bedrijf zelf.

Het kweken van awareness is een belangrijk punt, omdat zichtbaar wordt dat er veel mogelijk is met het vermarkten of verder gebruiken van persoonsgegevens. Om innovatieve en privacy-vriendelijke ontwikkelingen op dat gebied mogelijk te maken is het van belang dat er goed wordt nagedacht over de inrichting van processen, de waarborgen die worden geboden, de juridische kaders, en de wijze van communiceren naar de consument. Een 'zachte hand' gedurende het ontwikkeltraject is daarom zeer gewenst.

5.2 Kansen voor brancheorganisaties

Brancheorganisaties kunnen op veel punten een actievere rol spelen. In eerste instantie kunnen zij fungeren als informatiepunt op het gebied van privacyregelgeving en best practices om privacy te borgen in de bedrijfsvoering van organisaties. Een samenwerking tussen de brancheorganisaties kan een versterkend effect hebben, wanneer daardoor een branche-overstijgende aanpak ontstaat op het gebied van privacy. Belangrijker is mogelijk nog de functie waarin de brancheorganisatie uitdraagt dat privacy geen belemmering voor een productieve markt hoeft te zijn. In veel gevallen wordt privacy nog gezien als een showstopper. Of anders toch tenminste als een horde of een randvoorwaarde waaraan voldaan moet worden. Wanneer echter een positieve benadering wordt gekozen, is privacy een kans voor innovatie en kan het juist ook nieuwe diensten en mogelijkheden faciliteren. Om een dergelijke benadering breed gedragen te krijgen zijn de brancheorganisaties essentieel als communicatiekanaal naar hun achterban. Enkele voorlopers kunnen de kar gaan trekken, maar een branche brede aanpak is effectiever en kan sneller tot draagvlak leiden.

6 Interne factoren: gegevensbescherming als onderdeel van de bedrijfsvoering

Binnen bedrijven zelf kan gegevensbescherming een expliciete rol krijgen. Eén van de 'instrumenten' daartoe is de Functionaris voor de Gegevensbescherming (FG). Een organisatie kan een functionaris van de gegevensbescherming aanstellen, zoals aangegeven in artikel 62 Wbp, met bevoegdheden en taken zoals aangegeven in art 63 en 64 Wbp.[11] De FG geeft vorm aan een element van zelfregulering waarbij een organisatie kan volstaan de noodzakelijke melding van verwerking van persoonsgegevens aan de FG te doen in plaats van aan het Cbp. Aan een FG worden bepaalde eisen gesteld, zoals een voldoende kennisniveau van regels voor de bescherming van persoonsgegevens, sectorspecifieke wet- en regelgeving (afhankelijk van de sector waarin de FG opereert) en kennis van automatisering en ICT. Er zijn geen formele eisen gesteld aan de kennisachtergrond van een FG. Een FG dient een natuurlijk persoon te zijn (dus niet bijvoorbeeld een Ondernemingsraad) die een staffunctie vervult en wiens onafhankelijkheid ten opzichte van het bestuur/de directie van een organisatie gewaarborgd is. Een FG is een onderdeel van de invulling van de 'accountability' van een organisatie ten opzichte van de omgang met persoonsgegevens. De FG is de interne toezichthouder. Taken van de interne toezichthouder omvatten het in kaart brengen van processen binnen de organisatie waarin persoonsgegevens worden verwerkt, klachtenbehandeling, voorlichting en normontwikkeling binnen de organisatie. In sommige gevallen volstaat een melding van een gegevensbewerking bij de FG, in sommige gevallen (met name bij de bewerking van gevoelige gegevens) blijft een afzonderlijke meldplicht van de organisatie bij het CBP bestaan. Deze meldplicht is de verantwoordelijkheid van de verantwoordelijke en niet van de FG.

De FGs hebben zich verenigd in het Nederlandse Genootschap van Functionarissen voor de Gegevensbescherming. Dit Genootschap richt zich onder meer op bevordering van de kwaliteit en competenties van de FGs. Dit doet het door het aanbieden van documentatie, het organiseren van workshops en seminars en door leden te wijzen op vergelijkbare activiteiten op Europees niveau en bij andere organisaties. Het stelsel van de FGs zoals dit ook in de Data Protection Directive (95/46/EU) is weergegeven, is gebaseerd op de al langer bestaande Duitse aanpak rond intern toezichthoudende functionarissen. Het stelsel bestaat daar inmiddels al 55 jaar. Er is veel ervaring opgedaan met de vormgeving van intern toezicht binnen private organisaties.

Het CBP houdt een openbaar register bij van FGs. Op dit moment zijn daar FGs voor zo'n 360 organisaties ingeschreven. Sommige organisaties hebben meer dan één FG aangemeld (voor verschillende bedrijfsonderdelen), sommige FGs werken voor meer dan één organisatie. Het register bevat publieke en private instellingen. Het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming telt momenteel zo'n … leden. Het NGFG legt zich onder meer toe op belangenbehartiging van de leden, onder meer in de richting van het CBP. Uit een onlangs gehouden overleg tussen het NGFG en het CBP is overeengekomen dat het CBP de rol van de FG als verlengstuk erkent, en dat het CBP ook bereid is om de FGs directer bij te staan in de beoordeling van wat wel en wat niet is toegestaan in de omgang met persoonsgegevens. Op deze wijze wordt de slagkracht van het CBP vergroot en ontstaat een omvangrijker en geprofessionaliseerd net van toezichthouders.

[11] Zie www.cpbweb.nl en daarop beschikbare documentatie rond rol en verantwoordelijkheden FG; geraadpleegd 2 juli 2014

Naast de rol van het Genootschap in de vormgeving van de beroepsgroep zijn er andere interessante aanpakken die tonen dat het denken over privacy binnen organisaties langzaamaan volwassen wordt. Zo heeft op initiatief van Deloitte een achttal *privacy officers* zich verenigd in een informeel overlegorgaan dat zich toelegt op expertisebevordering en kennisdeling/-uitwisseling. De groep komt ieder kwartaal bij elkaar. Betrokken organisaties zijn Deloitte, KLM, KPN, NS, Philips, Rabobank, en TomTom. De agenda varieert per bijeenkomst maar is gericht op kennisdeling, het uitwisselen van ervaringen, en het signaleren van nieuwe ontwikkelingen. Niet alle *privacy officers* zijn geregistreerde FG'ers, reden om dit onderscheid tussen FG en *privacy officer* op deze plek te maken. De vraag is in hoeverre dit onderscheid in de toekomst een rol blijft spelen. De Article 29 Working Party heeft in een opinie over het omgaan met de meldingsplicht en de rol van de *data protection officers* aangegeven dat de *data protection officers* die bij organisaties zijn aangesteld een cruciale rol vervullen in het vergroten van de bewustwording in het omgaan met persoonsgegevens, en een van de redenen zijn die het welslagen van de werking van het wettelijk regime rond persoonsgegevens bepalen.[12] De aankomende Europese Algemene Verordening Gegevensbescherming[13] voedt deze positie van de FGs/*data protection officers*. Volgens de Verordening dienen alle organisaties die op jaarbasis gegevens verwerken van meer dan 5000 data subjecten een *DP officer* aan te stellen. Ook alle publieke organisaties die persoonsgegevens verwerken en organisaties die gevoelige gegevens verzamelen dienen een *DP officer* aan te stellen. De verordening schetst een aantal taken en bevoegdheden van de *DP officer*. Deze komen sterk overeen met de hierboven geschetste taken en bevoegdheden: onafhankelijk, staffunctie, directe rapportage aan de directie, en wat taken betreft het volgen van de verzameling, bewerking, opslag en verdere verwerking van persoonsgegevens binnen de organisatie, het opstellen van een overzicht, het bijdragen aan bewustwording van de verantwoordelijke en de verwerker, het informeren en adviseren van de verantwoordelijke en de verwerker, het bijhouden van conflicten, het fungeren als aanspreekpunt voor de nationale toezichthouder. Door de (verplichte) aanstelling van een *DP officer* is de meldingsplicht voor de organisatie te ondervangen en wordt ook terugdringing van administratieve lasten beoogd.

De professionalisering die hierboven is aangestipt, krijgt met de nieuwe verordening een nieuwe *boost*. Het aantal *DP officers* zal toenemen. Professionalisering van deze groep zal toenemen, hoewel in het begin aanloopproblemen te verwachten zijn in afstemming tussen vraag en aanbod. Een organisatie als het Nederlands Genootschap Functionarissen Gegevensbescherming zal een rol spelen in deze professionalisering. Daarnaast zijn initiatieven van *DP officers* zichtbaar zoals de ronde-tafelbijeenkomsten die we hierboven hebben aangehaald. Een ander initiatief is de in oprichting zijnde kennisportal voor privacy professionals van Verdonck, Klooster & Associates. Dit portal beoogt kennis bij elkaar te brengen over ontwikkelingen, tools en expertisebevordering voor de privacy professional. Een laatste onderdeel van de professionalisering van privacy professionals wordt geboden door de tijdschriften die zich op deze doelgroep richten. In Nederland is dat het tijdschrift Privacy & Informatie met een sterk juridische inslag en het vier jaar geleden opgerichte tijdschrift Privacy & Compliance, dat zich richt op de privacy professional.

---

[12] "Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union".WP 106, 10211/05/EN

[13] Officiële benaming General Data Protection Regulation (GDPR). Voor voorlopige tekst zie: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf .

7 Conclusies en aanbevelingen

In het project Actieplan Privacy is vanuit een brede blik gekeken naar de innovatie van privacypraktijken in Nederland. Er is een overzicht gemaakt van *best technologies* en *best practices*. Vervolgens is gekeken in hoeverre deze hun weg vinden naar de praktijk en welke andere factoren daar een belangrijke rol in vervullen (factoren als regelgeving, brancheorganisaties, *privacy officers*). Een aantal aansprekende voorbeelden van privacy-innovatiepraktijken is in het rapport uitgewerkt. De centrale vraag voor nu is hoe de aandacht voor privacy verder gebracht kan worden in het Nederlandse bedrijfslandschap. Welke kansen liggen er voor het verzilveren van een goede aandacht voor privacy in de bedrijfsvoering? Hoe draagt dit bij aan vooraanstaande positie voor Nederland op de internationale markt van privacyvriendelijke dienstverlening en de kansrijke benutting van privacy binnen bedrijven?

7.1 Conclusies

Een belangrijke eerste constatering is dat er in de praktijk van 'privacy als innovatie' al wel wat gebeurt, maar niet bijzonder veel. Er zijn absoluut mooie voorbeelden van praktijken waar privacy als uitgangspunt wordt meegenomen, maar het aantal voorbeelden is beperkt. Dat wil niet zeggen dat er geen interesse voor privacy is. Integendeel, de aandacht voor privacy is de afgelopen jaren sterk toegenomen. De opkomst, interesse en diversiteit van deelnemers aan de verschillende workshops en consultaties die in het kader van dit project zijn georganiseerd, geven aan dat het onderwerp leeft. De aandacht is er, maar de afstand tot concrete actie is nog te groot voor veel partijen. Slechts een beperkt aantal partijen neemt nadrukkelijk het voortouw.

Met de groeiende maatschappelijke aandacht voor privacy zou je meer concrete acties en initiatieven verwachten. Zeker nu er voldoende *best technologies* en *best practices* voorhanden zijn (zie de inventarisatie in Annex 3). In de workshops, de consultaties en de interviews gaven partijen echter aan dat ze privacytechnologieën te complex vinden of bang zijn dat benutting ervan ten koste gaat van de gebruiksvriendelijkheid van hun diensten. Daarnaast spelen andere factoren een rol in het achterblijven van een brede adoptie van degelijke technologieën.

Allereerst besteden niet alle bedrijven aandacht aan de mogelijke impact van hun diensten op de privacy van hun klanten, ze zijn er gewoonweg nog niet aan toe. Bij bedrijven die wel het belang hiervan inzien, en dit ook in hun bedrijfsvoering een plaats geven, zijn er vele die vooral gericht zijn op het voldoen aan de bestaande wet- en regelgeving. Proactief een stap verder zetten is er in die gevallen nog niet bij. Bovendien zijn er bedrijven en organisaties die signalen afgeven dat compliance al moeilijk genoeg is. Bedrijven ervaren de regelgeving met de bijbehorende vereisten als complex. Het meeste geldt dat voor de praktische uitwerking van de vereisten, dus het concreet operationaliseren van de wettelijke eisen. Bovendien is er vaak sprake van een gebrek aan bewustzijn dat persoonsgegevens worden verwerkt en dat daar een wettelijk kader voor geldt. Dat is bijvoorbeeld het geval omdat er het idee is dat de verwerking zo vanzelfsprekend is dat daar geen aparte vereisten voor gelden, zoals bij het verwerken van klantgegevens of andere contactgegevens. In andere gevallen is de reikwijdte van het begrip persoonsgegeven niet bekend, zodat bijvoorbeeld een IP-adres of klantnummer niet als zodanig wordt herkend. Positieve

Bedrijven ervaren regelgeving als complex

Markt voor juridische dienstverlening komt tot ontwikkeling

constatering is dat de markt voor juridische dienstverlening op het gebied van privacy compliance over de afgelopen jaren tot wasdom is gekomen. Deze markt functioneert, en er zijn geen signalen dat dit nadere ondersteuning of aandacht behoeft.

Wel is duidelijk geworden dat compliance hoofdzakelijk juridisch wordt benaderd. Technische implementatie of ondersteuning is nog ondergeschikt. Dit heeft mogelijk te maken met het feit dat het voldoen aan wetten en regels in de meeste gevallen gerealiseerd kan worden met organisatorische en juridische maatregelen, en niet veel extra technologie vereist, dus ook geen specialistische privacytechnologie. Er wordt bijvoorbeeld eenmalig aandacht besteed aan compliance, door de meldingen bij het Cbp in orde te maken en enkele organisatorische afspraken over bijvoorbeeld bewaartermijnen vast te leggen. Er is echter geen sprake van een structurele aanpak in de organisatie als geheel. In combinatie met de juridische invulling is privacy dan ook nog vaak onderdeel van een bedrijfsmatige risicoafweging. Kosten en baten worden tegen elkaar afgewogen. In het huidige speelveld zijn er veel partijen voor wie volledige compliance mogelijk conflicteert met het business model dat gehanteerd wordt. Gezien de economische baten van exploitatie van persoonsgegevens valt de risicoafweging dan ook vaak uit in het nadeel van een goede bescherming van de privacy. Er is alleen expliciete aandacht voor privacy bij commerciële kansen met winst of bij incidenten. De beperkte middelen van de toezichthouder (College bescherming persoonsgegevens) en daarmee de geringe pakkans zijn daar mogelijk ook debet aan.

Privacy wordt voornamelijk als juridisch risico benaderd

Beperkte aandacht voor privacy als innovatie bij systeem-aanbieders

Belangrijker in dit verband echter is de conclusie dat privacy nog niet vanzelfsprekend als een kans wordt gezien, als een mogelijkheid om zich positief te profileren. Privacy vindt nog nauwelijks een weg in de business proposities van bedrijven. Dat persoonsgegevens een zekere waarde vertegenwoordigen wordt breed erkend. De gedachte dat die waarde ook in de bescherming van die gegevens kan zitten is minder prominent vertegenwoordigd. Het aanbod van privacy-technologieën vanuit de grote technologiebedrijven blijft ook nog beperkt. Een aantal van deze bedrijven participeert wel actief in Europese onderzoeksprojecten en ontwikkelt intern nieuwe toepassingen of technologieën, maar de weg naar de markt wordt niet gevonden. Het aanbod van privacy-technologie is doorgaans ook niet duidelijk aanwezig in het productportfolio op de websites van de grote aanbieders.

Tot slot is er een grote groep bedrijven die hun business haalt uit de handel in persoonsgegevens (*online marketing* bedrijven, *data brokers*, *data analytics* bedrijven). In hun optiek is bescherming van de privacy een hindernis voor verdere uitbouw van hun dienstverlening. Een belangrijk deel van de gegevens die deze bedrijven verzamelen komt uit ‘observed data’ (zie WEF, 2014) waarvan de klant nauwelijks weet heeft dat deze verzameld worden. Voor deze bedrijven is de overgang van een business model dat gebaseerd is op beschikbaarheid van en handel in persoonsgegevens naar een business model waarin bescherming van de privacy van een individu ook meerwaarde oplevert, een

erg grote en – op grond van de ontwikkelingen rond *big data* en *big data analytics* – ook niet de meest vanzelfsprekende.

7.1.1 De ontwikkeling van een privacy speelveld

Ondanks de gesignaleerde belemmeringen die adoptie van privacytechnologieën in de weg staan, ontstaat er een privacy speelveld met een aantal centrale elementen . Ten eerste blijkt innovatie op het gebied van privacy en privacyvriendelijke dienstverlening voor een belangrijk deel plaats te vinden vanuit innovatieve start ups. Het gaat om bedrijven die een niche hebben gevonden en daar specifieke diensten en oplossingen bieden die privacy en controle over gegevens door het data subject als uitgangspunt hebben. CV-OK is hier een goed voorbeeld van. Kennelijk is er een vraag naar geverifieerde informatie op CV's van sollicitanten, met name in de financiële sector waar specifieke screenings wettelijk vereist zijn en tegelijkertijd veel verloop plaatsvindt vanwege de inzet van flexwerkers en interim krachten. CV-OK heeft daarop een dienst ingericht waarmee de screenings betrouwbaar plaats kunnen vinden en richt zich nu op het beheer van een digitaal CV door het data subject in de vorm van YOPS.

Belangrijke rol innovatieve start-ups

Naast CV-OK positioneren bedrijven zoals Synergetics en Ixquick en een stichting zoals Qiy Foundation zich als spelers die innovatieve benaderingen van het omgaan met privacy voorstaan en verder willen gaan dan alleen het aanbieden van middelen om compliance te realiseren. Binnen de meer gevestigde orde zijn ook bedrijven te vinden die een dergelijke insteek kiezen, en hier ook actie op ondernemen. NS is daar een voorbeeld van, zoals in dit rapport uiteengezet. Maar ook Ziggo heeft recent een aantal initiatieven genomen, bijvoorbeeld door het aanstellen van zo'n 50 Privacy Champions: mensen op de werkvloer die verantwoordelijk zijn voor het naleven van privacy regelgeving, het belang van privacy uitdragen, en een eerste aanspreekpunt zijn voor vragen of opmerkingen. Deze praktijk is een goed voorbeeld van hoe een organisatie stappen kan zetten om een breed draagvlak in alle lagen van het bedrijf te creëren.

Interessante initiatieven van gevestigde bedrijven

7.1.2 Inspelen op privacy

In dit speelveld zijn drie belangrijke perspectieven te onderscheiden waarbij privacy in bestaande en in nieuwe processen en systemen wordt opgenomen.

1. Privacy als service enabler
2. Privacy als niche
3. Privacy als compliance

Privacy als service enabler verwijst naar manieren om nieuwe diensten privacyvriendelijk in te richten, maar ook om nieuwe diensten mogelijk te maken. We zijn hier verschillende voorbeelden van tegengekomen, zoals bij de NS, Ziggo en TomTom.

Privacy als niche wijst op de innovatieve start-ups die zich richten op een aanbod van privacyvriendelijke diensten. Dit zijn bedrijven wiens productportfolio bestaat uit privacyvriendelijke diensten, producten en systemen. CV-OK past in deze categorie, evenals een bedrijf als Synergetics met zijn trust frameworks en Qiy met zijn datakluisinitiatieven.

Bij deze eerste twee perspectieven wordt privacy als kans gezien, en worden nieuwe mogelijkheden om privacyvriendelijke producten en diensten te ontwikkelen en in te voeren verkend. In de derde benadering, *privacy als compliance*, is meer sprake van privacy als een voorwaarde waar noodzakelijkerwijs aan voldaan moet worden, maar niet altijd van harte. Hier liggen wel kansen voor juridische dienstverleners, en dit blijkt in de praktijk al tot een functionerende markt te hebben geleid. Privacy Impact Assessments en ondersteuning bij compliance worden door een aantal gespecialiseerde consultancy bedrijven aangeboden en ontwikkeld.

Naast deze drie perspectieven dient nog een perspectief vermeld te worden. Dit is het perspectief waarin het business model afhankelijk is van het verzamelen en verder verwerken van persoonsgegevens. In deze categorie vallen bijvoorbeeld *online* adverteerders, sociale netwerkaanbieders en *data brokers*. Privacy wordt binnen deze categorie niet als kans gezien, maar meer als een hinderende factor. Regelgeving kan beperkend werken op de zakelijke mogelijkheden voor deze bedrijven. Hier manifesteert zich de spanning tussen commercieel en maatschappelijk belang. Regulering en handhaving bieden in dit geval een kapstok om de privacy van burgers en consumenten te beschermen. Daarnaast zijn er ook bij deze bedrijven kansen aan te geven in het omgaan met privacy. Dit vraagt om een radicale herziening van de bedrijfsprocessen en de organisatorische benadering van persoonsgegevens. Ook hier zijn voorbeelden van te geven, geïnitieerd en ondersteund door privacy-als-niche bedrijven.

Sommige bedrijven hebben geen belang bij bescherming van privacy

Het is gebleken dat privacy innovatie grotendeels afhankelijk is van de bedrijfscultuur. Om privacy daadwerkelijk vorm te geven moet het een prominente plaats innemen in de dagelijkse gang van zaken. Bekendheid met het onderwerp en positieve aandacht voor privacy zijn daartoe noodzakelijk. Een brede aanpak waarmee in het algemeen het besef van het belang van privacy groeit en waarin ook de kansen die privacy voor bedrijven brengt goed naar voren komen is dus essentieel.

7.1.3 Benutting en uitbouw van de kansen

Voor het wegnemen van belemmeringen en het verder stimuleren van de markt van vraag en aanbod rond privacy als kans zien wij verschillende mogelijkheden:

Rol brancheorganisaties

Zo kunnen brancheorganisaties en het ECP zorgen voor een brede verspreiding van kennis en praktijken op het gebied van privacy innovatie. Zoals in dit rapport getoond hebben verschillende organisaties een dergelijke rol op zich genomen. De uitwerking daarvan en de activiteiten die daaraan zijn gekoppeld (algemene voorlichting, gerichte bijeenkomsten, of concrete handleidingen) verschillen echter sterk. Een actieve houding waarin privacy als kans wordt uitgedragen is gewenst.

Rol privacy officers

Ook het benoemen van goede privacy officers binnen een organisatie kan een bijdrage leveren. Dit is onder meer te zien in de voorbeelden van NS en Ziggo. In de aankomende Algemene Verordening Gegevensbescherming wordt voor veel organisaties een functionaris gegevensbescherming zelfs verplicht gesteld. Essentieel is niet alleen de aanstelling van een privacy officer, maar ook een hierop ingerichte organisatie met een positief ingestelde top. Dat betekent in de praktijk dus ook dat de privacy officer daadwerkelijk bevoegdheden en doorzettingsmacht toebedeeld moet krijgen. Ook in dit geval moet privacy als kans worden gezien en niet alleen als een juridische barrière die innovatie hindert.

Rol kennisinstellingen

Er is een belangrijke rol weggelegd voor kennisinstellingen. Deze partijen zijn in staat tot het verder ontwikkelen en ontsluiten van technologische oplossingen. Daarnaast kunnen zij bijdragen aan het ontwikkelen van toekomstvisies, het plaatsen van innovatie in relatie tot maatschappelijke ontwikkelingen, en het ontwikkelen van nieuwe business modellen gebaseerd op privacy.

Rol juridisch kader

De reeds genoemde Algemene Verordening Gegevensbescherming acteert ook als een belangrijke driver. Verschillende bestaande concepten worden verder uitgewerkt en nieuwe concepten worden toegevoegd aan het juridisch kader. In dit verband zijn vooral Data Protection by Design en Privacy by Design van belang, maar ook de nadere bepalingen op het gebied van bijvoorbeeld profileringstechnologie kunnen een aanleiding vormen voor verdere privacy-innovatie. Daarnaast zal ook de rol en positie van de toezichthouder versterkt worden. Striktere handhaving is daarmee ook te verwachten, wat kan bijdragen aan het serieuzer oppakken van privacy binnen organisaties.

Rol overheid

Dan de rol van de overheid: met de overgang van een aantal taken naar gemeenten (bijvoorbeeld op het gebied van zorg) bestaat het risico dat vele partijen zelf het wiel uit gaan vinden waar het gaat om de omgang met en het beheer van persoonsgegevens. De – centrale – overheid heeft hier een kans door over gemeenten heen initiatieven te stimuleren en te belonen die bijdragen aan een goede en innovatieve verankering van privacy in de bedrijfsvoering. Bepaalde nichespelers richten zich op deze markt. Ondersteuning van deze initiatieven kan leiden tot synergie en meerwaarde voor gemeenten.

Landelijke initiatieven

Op landelijk niveau zijn er eveneens initiatieven die zich richten op innovatieve aanpakken rond omgang met persoonsgegevens. Het Big Data Value Centre in Almere is hier een voorbeeld van. Ondersteuning door de centrale overheid van deze initiatieven in concrete acties kan bijdragen aan een verspreiding van *best technologies* en *best practices* rond omgang met persoonsgegevens.

De algemene uitdaging ligt dus in het uitdragen van privacy als een kans voor innovatie. Op dit moment is er bij de meeste organisaties nog weinig ervaring met het inbedden van privacytechnologie in de bedrijfsvoering. Dat betekent dat er dus ook gekeken moet worden naar manieren om reeds aanwezige kennis effectief te maken.

7.2 Aanbevelingen

Op basis van bovenstaande conclusies kan een aantal aanbevelingen geformuleerd worden over de rol die het ministerie van Economisch Zaken kan spelen. Deze worden hieronder benoemd.

7.2.1 Bevorderen van continue dialoog: ervaringen en nieuwe kansen

Een eerste aanbeveling is het faciliteren van een **structureel platform** voor het bij elkaar brengen van kennis en ervaringen. Het is belangrijk om de nog steeds heersende onbekendheid met aanpak van privacyvraagstukken en de benutting van – geavanceerde – privacytechnologieën aan te blijven pakken via gerichte activiteiten. Het verspreiden van kennis en ervaringen is een noodzakelijke voorwaarde om privacy-innovatie in Nederland een stap verder te brengen.

Betrokken partijen: Binnen een dergelijk platform dienen verschillende partijen bij elkaar gebracht te worden. Niet alleen individuele bedrijven, maar ook brancheorganisaties,

vertegenwoordigers van kennisinstellingen, privacy officers, privacy-activisten en aanbieders van technologieën en systemen.

Doel van het platform is een systematische monitoring van privacy-praktijken, het vergroten van de *awareness* voor deze praktijken in de buitenwereld, en het delen en verspreiden van kennis en ervaringen over invoering van privacy-praktijken.

Werkwijze: Het privacy platform kan gevraagd worden om advies inzake vraagstukken rond de maatschappelijke inbedding van privacy. Het platform kan ook zelf advies uitbrengen.

Rol Economische Zaken: Het ministerie van Economische Zaken is de initiator van het platform, en ondersteunt het platform financieel (secretariaat, budget voor awareness activiteiten).

7.2.2 Nieuwe kennisontwikkeling

Naast het verspreiden van kennis en ervaringen is het verder ontwikkelen van kennis ook noodzakelijk. Ontwikkelingen op het gebied van gegevensverwerkingen, beveiliging van gegevens en bedreigingen voor de veiligheid van gegevens nopen tot een continue agenda voor privacytechnologie en privacy-vriendelijk innoveren. Dit geldt eens te meer indien Nederland zich wil profileren op het gebied van privacy als innovatie. Om dit te bewerkstelligen is **investeren in kennis en kennisontwikkeling** vereist.

Betrokken partijen: NWO en STW zijn – samen met de beheerders van de roadmap ICT – de eerste aanspreekpunten om een gerichte impuls te geven aan de verdere kennisontwikkeling. Binnen de roadmap ICT biedt de actielijn 'Vertrouwen in ICT' een concreet aangrijpingspunt, met een rol voor zowel ICT in als voor de topsectoren. Ook een apart EZ-programma Privacy als innovatie behoort tot de mogelijkheden.

Doel: Het investeren in nieuwe kennisontwikkeling rond privacy met het oog op innovatieve oplossingen die economisch en maatschappelijk renderen.

Werkwijze: Specifieke agendering van Privacy in calls binnen NWO/STW; specifiek programma Privacy als innovatie binnen innovatie-activiteiten EZ.

Rol Economische Zaken: Invloed aanwenden voor aandacht privacy binnen NWO-STW activiteiten; opzetten eigen innovatieprogramma 'Privacy als Innovatie'.

7.2.3 Opstellen van een privacy-benchmark

Veel bedrijven zijn zoekende naar een adequaat niveau van privacybescherming in hun bedrijfsvoering. Enerzijds kan dit betekenen dat voldaan wordt aan de eisen die de Wet bescherming persoonsgegevens en de komende Verordening stellen. Anderzijds is compliance slechts een eerste stap om in een vertrouwensvolle relatie met klanten te komen. Het **opstellen van een benchmark** die bedrijven in staat stelt hun positie in maturiteit te bepalen ten opzichte van organisatorische, bedrijfsmatige en systeemtechnische maatregelen kan helpen om het privacybewustzijn te vergroten in relatie tot de na te streven klantrelatie. Een aanzet voor een dergelijke benchmark is te vinden in het bestaande Privacy Maturity Model. Dit model richt zich vooral op organisatorische maturiteit. Aanvulling van deze benchmark met bedrijfsmatige en systeemtechnische maatregelen kan bedrijven helpen bij het vaststellen van hun eigen actieplan om privacy in de bedrijfsvoering op

te nemen. Tegelijkertijd draagt een benchmarkonderzoek bij aan privacy als agendapunt binnen het bedrijfsleven. Daarmee kan ook de bedrijfscultuur enigszins gestuurd worden.

Betrokken partijen: een partij dient uitgenodigd te worden om de benchmark te ontwikkelen.

Doel: Bieden van duidelijke richtlijnen met betrekking tot inbedding van privacy in bedrijfsvoering; ontwikkeling van bewustwording en standaarden.

Werkwijze: In eerste instantie ontwikkeling; vervolgens test en uitzetten van privacy-benchmark via brancheorganisaties en andere gremia.

Rol Economische Zaken: faciliteren van ontwikkeling benchmark; stimuleren toetsing en invoering.

7.2.4 Ondersteunen van innovatieve start-ups

Een vierde aanbeveling betreft het **(financieel) ondersteunen van innovatieve start-ups** met de verdere ontwikkeling en verspreiding van hun aanpak. In de regel bieden deze innovatieve bedrijven hun diensten aan aan derde partijen. Dit zijn kosten- en tijdsintensieve trajecten. Bij radicale innovatie ten opzichte van de bestaande aanpak zal een bedrijf meer te overwinnen hebben om de mogelijkheden die een innovatieve start-up biedt in de bedrijfsvoering op te nemen (initieel als *testbed* of *proof of concept*).

Betrokken partijen: Ministerie van Economische Zaken, en hierbij behorende organisaties (zoals Rijksdienst voor Ondernemend Nederland en Syntens); brancheorganisaties (VNO-NCW, Nederland ICT).

Doel: Vergroten kansen van innovatieve start-ups om nieuwe privacydiensten en –producten te vervolmaken en te vermarkten. Vergroten aantrekkelijkheid voor start-ups om zich in deze markt te begeven.

Werkwijze: Gerichte financiële ondersteuning vanuit het ministerie kan bedrijven helpen om privacypraktijken te beproeven en kan innovatieve start-ups ondersteunen in de uitbreiding van bedrijfsactiviteiten. Deze financiering kan onderdeel zijn van al bestaande innovatie-instrumenten (onder meer bij Syntens) maar het lijkt raadzaam om hier prestatieafspraken over te maken en regels op te stellen voor de benutting van al bestaande fondsen. Waar mogelijkheden zijn om deze fondsen op te tuigen met aanvullende financiële middelen zou dit ook overwogen moeten worden.

Rol Economische Zaken: Aanjagen opzet ondersteuning innovatieve start-ups; beschikbaarstelling van financiën.

7.2.5 Organiseren Privathon

Om privacy-innovatie verder te stimuleren kan ook een jaarlijkse **Privathon** (een hackaton op privacygebied) georganiseerd worden. Net zoals bij een Hackathon wordt bij een Privathon een privacyprobleem centraal gesteld en worden onderzoekers en andere geïnteresseerden uitgenodigd om een oplossing te ontwikkelen en te presenteren.

Betrokken partijen: organisatie die voor Economische Zaken de praktische uitwerking van de Privathon verzorgt.

Doel: De Privathon heeft tot doel om onderzoekers te betrekken bij het vinden van oplossingen voor specifieke privacyvraagstukken en heeft als afgeleid doel om de mogelijkheden om dit met technische oplossingen verder te brengen onder de aandacht te brengen. Als positieve stimulans kan gedacht worden aan het instellen van een 'Kans op Privacy'-award voor de organisatie die demonstreert hoe het 'Privacy als kans' heeft ingebed in zijn bedrijfsvoering.

Werkwijze: Jaarlijkse organisatie, met wisselende opdrachten; instellen jury, organiseren van een prijsvraag; beschikbaarstelling van een award.

Rol Economische Zaken: Initiatiefnemer; bijdrage aan financiering van de Privathon.

7.2.6 Overheid als *launching customer*

Verder kan de overheid zelf een voorbeeldfunctie vervullen en bij onderdelen van programma's van andere ministeries (dan Economische Zaken) aandacht vragen voor een privacyvriendelijke benadering en voor de uitwerking van privacyvriendelijke innovatiepraktijken. In dit geval acteert de **overheid als *launching customer***, geeft zelf het goede voorbeeld, en biedt het zichzelf als lerende omgeving aan waar andere partijen van kunnen profiteren.

Betrokken partijen: Voor de hand liggende departementen zijn Volksgezondheid, Welzijn en Sport (met name rond ontwikkelingen in de zorg), het Ministerie van Veiligheid en Justitie (rond vraagstukken die de openbare orde betreffen) en het ministerie van Infrastructuur en Mobiliteit (rond opslag van gegevens in het OV, en cameratoezicht op wegen).

Doel: Invulling geven aan 'Practice what you preach'. Stimuleren rijksbrede bewustwording van mogelijkheden voor privacyvriendelijke innovatie. Aanjagen van privacy als innovatie.

Werkwijze: Onderzoeken binnen welke overheidsprogramma's 'Privacy als innovatie' kan worden ingebracht. Dialoog aangaan om privacy in deze programma's in te bedden.

Rol van Economische zaken: Initiërende en coördinerende rol.

7.3 Tot slot, verhogen compliance en beschermingsniveau

Met het oog op de bestaande praktijk waaruit blijkt dat er ook partijen zijn die vanuit hun business model juist geen belang hebben bij privacy, ligt het voor de hand dat er nog steeds een belangrijke rol is weggelegd voor regelgeving en handhaving. De aankomende Algemene Verordening Bescherming Persoonsgegevens vormt daar een belangrijke stap in. Een aantal juridische vereisten wordt aangescherpt en ook op het gebied van handhaving lijken meer bevoegdheden en mogelijkheden te ontstaan. Hoewel er ook binnen deze categorie voorbeelden zijn van bedrijven die privacy op een innovatieve manier verbinden met hun business aanpak, zal een groot deel van de bedrijven minder kansen zien in het stimuleren van privacyvriendelijke innovatie. Met juridische kaders en adequate handhaving kan echter wel het algehele beschermingsniveau ten aanzien van privacy verhoogd worden. In het verlengde daarvan kan gedacht worden aan het breder trekken van compliance, bijvoorbeeld door de noodzaak voor bedrijven om zich aan de wet te houden explicieter neer te zetten, mogelijk in combinatie met een benchmark (zie aanbeveling 3).

Annex 1: Opzet en pitches workshop regelgeving

Privacy innovaties en maatschappelijke implementatie

1. Inleiding

Privacy staat onder druk door moderne ICT. Om privacy te waarborgen binnen onze maatschappij moet er 'iets' gebeuren. Uitgangspunt in dit hoofdstuk is dat gebruik gemaakt zou moeten worden van bestaande privacy innovaties die in zogenaamde 'Best Practices' hun nut bewezen hebben. Een aantal van deze privacy innovaties zijn geïdentificeerd binnen het eerdere desk research binnen het Actieplan Privacy. Echter identificatie van dergelijke innovaties is niet afdoende, de vervolgvraag is: *"Hoe kunnen we realiseren dat deze privacy innovaties daadwerkelijk binnen de maatschappij opgepakt worden?"* Deze vraag heeft als uitgangspunt gediend bij de workshop waarop dit hoofdstuk gebaseerd is. Het doel van de workshop was helderheid te krijgen over de 'driving forces' en randvoorwaarden voor de acceptatie en implementatie van privacy innovaties en de rol die de huidige wet- en regelgeving hierin speelt. Door de focus op het wettelijk kader, kan de hoofdvraag meer toegespitst verwoord worden als: *"Biedt het huidige wettelijk kader voldoende incentives om privacy-innovaties te stimuleren?"*

2. Workshop

2.1 Deelnemers

De betreffende workshop is gehouden is op 26 mei 2014 bij TNO Delft. Bij deze workshop waren de volgende personen aanwezig: Roman Volf (EZ), André Biesheuvel (Duthler Associates), Ronald Leenes (TILT), Colette Cuijpers (TILT), Arnold Roosendaal (TNO), Marc van Lieshout (TNO), Ot van Daalen (Digital Defence), Friederike van der Jagt (Stibbe), Hans de Zwart (BOF), Bart van der Sloot (IVIR), Linda Kool (Rathenau Instituut), Thomas van Essen (SOLV).

2.2 Opzet

De opzet van de workshop was als volgt. Eerst zijn vanuit een aantal verschillende perspectieven een aantal korte pitches gegeven. Friederike van der Jagt heeft een pitch verzorgd vanuit het perspectief van de praktijk, Hans de Zwart vanuit het burgerperspectief, André Biesheuvel vanuit het marktperspectief, en Bart van der Sloot en Ronald Leenes hebben een pitch verzorgd vanuit het perspectief van het regulerend kader. Na deze ronde van pitches is eenieder om een reactie verzocht, waarna de discussie, onder leiding van Ronald Leenes, zich heeft toegespitst op enkele van de kernbevindingen uit de pitches en de reacties daarop. De workshop is afgesloten met een laatste ronde waarin alle deelnemers, desgewenst, de voor hen meest belangrijke bevindingen van de workshop nog eens voor het voetlicht konden brengen.

2.3 Input en voorbereiding

Voorafgaand aan de workshop is aan de deelnemers naast de centrale vraag en de sub-vraag enige achtergrondinformatie ter beschikking gesteld en zijn de vragen geponeerd in een spectrum met twee uitersten. Aan de ene kant van het spectrum de stelling: *"De huidige regelgeving zet de markt aan om zelf te innoveren. Er is geen behoefte aan aanvullende regelgeving of enige andere maatregelen (stimuleringsmaatregelen, zoals belastingvoordelen, subsidies, o.i.d.) vanuit overheid".* En aan de andere kant van het spectrum de stelling: *"Het huidige wettelijke kader biedt onvoldoende tegenwicht aan het gebrek aan een level playing field, hetgeen een deal breaker is voor het slagen van privacy-innovatie" of, anders verwoordt: "Er is nu eenmaal een spanningsveld tussen de datahongerigen en burgers/consumenten. Zolang de hongerigen belang houden bij data zal PET en PbD niets worden, tenzij je ze dwingt met wet- en regelgeving".*[14]

Naast de centrale vraag die is voorgelegd aan de inleiders: *"Hoe bij te dragen aan acceptatie en implementatie van privacy innovaties en welke rol speelt het huidige wettelijke kader hierin, of zou het huidige wettelijke kader hierin moeten spelen"?* Is voor elk perspectief een lijstje met vragen opgesteld ter inspiratie. Deze vragen zijn niet alleen toegestuurd aan de inleiders, maar aan alle deelnemers aan de workshop. Het gaat om de volgende inspiratie vragen:

<u>Innovaties:</u>

Hoe kunnen karakteristieken van innovaties bijdragen aan de acceptatie en implementatie van de innovatie binnen de maatschappij?

Welke randvoorwaarden zijn van belang bij het landen van een innovatie in de praktijk?

Draagt de huidige regelgeving voldoende bij aan het teweegbrengen van privacy-innovatie?

Zijn er aanvullende maatregelen nodig en zo ja vanuit welk juridisch domein en in welke vorm, wet- en regelgeving of zelfregulering?

<u>Bedrijven/praktijk:</u>

Is er een business model voor privacy innovaties?

Zo nee, hoe creëer je een business model voor privacy innovaties?

Kan dit geheel vanuit de markt gestimuleerd worden, of is hier de betrokkenheid van andere partijen bij nodig?

Is er überhaupt een markt voor privacy innovaties?

[14] PET: Privacy Enhancing Technologies. PbD: Privacy by Design.

Zo nee, wat zijn de randvoorwaarden om een dergelijke markt te kunnen creëren?

Draagt de huidige regelgeving voldoende bij aan het teweegbrengen van privacy-innovatie vanuit de markt?

Zijn er aanvullende maatregelen nodig en zo ja vanuit welk juridisch domein en in welke vorm, wet- en regelgeving of zelfregulering?

Burgers/Consumenten:

Waarom stellen consumenten geen eisen aan producten en diensten?

Onder welke omstandigheden doen zij dit wel?

Hoe kunnen consumenten een drijvende rol spelen bij de acceptatie en implementatie van innovaties?

Geeft de huidige regelgeving de burger/consument voldoende middelen in handen om privacy-innovatie (mee) af te dwingen?

Zijn er aanvullende maatregelen nodig en zo ja vanuit welk juridisch domein en in welke vorm, wet- en regelgeving of zelfregulering?

Overheid:

Moet de overheid een laissez-faire aanpak voorstaan, en het aan de markt overlaten?

Moet de overheid participeren, samenwerking zoeken met de markt?

Moet de overheid actief sturen, door middel van wet- en regelgeving?

Wat zijn argumenten voor en tegen de genoemde benaderingen?

Tot slot is aan alle deelnemers van de workshop ter voorbereiding een zestal stellingen voorgelegd:

1. De overheid moet de acceptatie en implementatie van privacy innovaties wettelijk verplicht stellen.

2. De overheid heeft een positieve verplichting om bij te dragen aan de bescherming van fundamentele waarden.

3. De markt moet geheel vrij gelaten worden aangezien er genoeg ‘driving force’ binnen de markt zelf is voor de landing van privacy innovaties.

4. Je kunt het niet aan de markt overlaten, want er is geen markt.

5. 'Consumer empowerment' is noodzakelijk zodat privacy innovaties vanuit de vraagzijde gestimuleerd kunnen worden.

6. Van de consument kun je niets verwachten door de scheve machtsverhouding in de markt.

3. Pitches

3.1 Pitch Friederike van der Jagt

De eerste pitch is gegeven door Friederike van der Jagt, advocate bij Stibbe. Uitgangspunt in haar pitch is dat het wettelijk kader niet altijd de boosdoener is. Het gaat om de vraag wat wij als maatschappij wenselijk achten om op te leggen aan partijen. Bedrijven hebben een veel lager kennisniveau van privacy dan wij denken. Privacy en dataprotectie vormen geen prioriteit, tenminste niet tot het moment dat er boetes zijn, actieve handhaving te verwachten valt en/of reputatieschade, of wanneer het echt een unique selling point kan zijn. Interesse voor privacy in het bedrijfsleven is beperkt, en het (technische) begrippenkader is grotendeels onbekend in het bedrijfsleven. Er zijn veel open normen en daarom zijn er bepaalde standaarden, op bepaald technisch niveau, noodzakelijk. Wij juristen kleuren open normen heel anders in dan hoe bedrijven dit doen. Bedrijven vinden veel gegevensverwerkingen noodzakelijk, en al snel zijn bedrijven overtuigd van anonimisering terwijl daar juridisch gezien geen sprake van is, en een belangenafweging op basis waarvan bedrijven persoonsgegevens zouden mogen verwerken valt al snel uit in het voordeel van het bedrijfsleven. Er is op deze vlakken handzame uitleg nodig. En ook bij de consument ligt een probleem want die hebben geen enkel idee waar ze toestemming voor geven. Ze kunnen ook geen kant op en zijn niet in staat de markt te veranderen richting meer privacy vriendelijke diensten en producten. Daarom moeten veel strikter standaarden en voorwaarden verplicht worden opgelegd via wetgeving. Daar zal dan wel weerstand tegen zijn in het begin, maar het heeft uiteindelijk wel effect. Open normen leveren veel werk op voor juristen, maar geven geen rechtszekerheid of verbetering van privacybescherming. Ook moet de overheid ingrijpen op het gebied van gelaagde toestemming (layered consent). Veel oplossingen zijn deeloplossingen. BCR's bijvoorbeeld lossen een intern bedrijfsprobleem op bij multinationals, maar hebben geen effect op de relatie bedrijf-externe omgeving. Innoverende partijen moeten worden gestimuleerd, maar moeten ook handvatten krijgen zodat ze weten wat ze moeten doen, zodat privacy niet meer een irritatie is maar daadwerkelijk kan uitmonden in een unique selling point.

3.2 Pitch Hans de Zwart

Hans de Zwart, voorzitter van de burgerrechtenbeweging Bits of Freedom, begint zijn pitch met een verwijzing naar de Snowden-affaire en de toename in burgerbewustzijn die hierdoor teweeg is gebracht. BOF merkt dit op allerlei manieren, stijging donaties, drukbezocht checkpoint op bevrijdingsfestival waar mensen de beveiliging van hun telefoon konden controleren. Ook de zogenaamde Privacy-cafés worden steeds drukker bezocht. Ook bij deze bijeenkomsten staat centraal hoe je als burger je email kunt beveiligen en hoe je trackers kunt vermijden. Dit heeft echter

twee kanten, het is goed dat consumenten bewust worden dat technologie niet neutraal is, maar aan de andere kant wordt duidelijk dat mensen de technologie gewoon echt niet snappen. Ze installeren namelijk blindelings wat er door BOF voorgedragen wordt. We moeten niet willen leven in een wereld waar we zelf verantwoordelijk zijn voor onze privacy en waar we zelf maatregelen moeten nemen omdat we derde partijen niet langer vertrouwen, zoals bijvoorbeeld wekelijks 500 euro pinnen en dan alles cash betalen omdat dit moelijker te traceren is, of met een masker op over straat om herkenning te voorkomen. BOF merkt dat bedrijven privacy steeds meer zien als markt, maar dat het dan vaak gaat om totaal valse claims betreffende privacybescherming. Bedrijven hebben geen enkele incentive om privacyvriendelijk te zijn, en dus moeten we dingen gewoon niet langer toestaan, zeker niet aangezien de burger zelf te weinig kennis heeft om zich deugdelijk te beschermen met te softe mechanismen zoals toestemming.

3.3 Pitch André Biesheuvel

De pitch van André Biesheuvel vertrekt vanuit een economisch perspectief en stelt als uitgangspunt dat er ergens een business case moet zijn zodat actoren een incentive hebben om iets te gaan doen. Wetgeving is bedoeld om normadressaten te beïnvloeden. Als we makro economisch naar de markt kijken, is er duidelijk een mate van informatie imperfectie. Als voorbeeld van een volmaakt imperfecte markt kan gewezen worden op de staat, als zijnde monopolist. Het gaat dus om informatie-asymmetrie en de vraag is waarom er imperfecte markten blijven bestaan – bijvoorbeeld in de financiële sector –, want iemand in dit stelsel betaalt hier de prijs voor. Interbancair rekenen banken elkaar bijvoorbeeld 0,3 procent rente, maar een rekening courant schommelt tussen de 6 en 11 procent. Een groot percentage betreft het overeind houden van de markt, maar een deel komt ook omdat ‘men de klant niet kent’. Om dit probleem aan te pakken is een heel apparaat aan regelgeving ingesteld om de klant te leren kennen, maar kennelijk levert het niet kennen van je klant meer op in deze markt, dan het wel kennen van de klant. Je kunt beter een risicopremie op je rente leggen.

Bij imperfecte informatie ecosystemen bestaat er voor bedrijven en instellingen een perverse prikkel om die imperfecte markt in stand te houden. In geval van marktimperfecties ligt er wel voor bedrijven een risico op sancties, of aansprakelijkheid. De omvang van die sancties is bepalend voor het gedrag van de actoren. We moeten dan ook zeer verheugd zijn over de verhoging van de sanctiebesluiten in de voorgestelde Privacy Verordening, meer hoeft de regelgever eigenlijk niet te doen. Als je vanuit de technologie naar Big Data en cloud computing kijkt is er nog steeds een perceptie dat informatie gratis is. Dat is onjuist, informatie is een liability. Het hebben van informatie impliceert dat deze een bepaalde kwaliteit moet hebben anders is het sanctiewaardig. Een voorbeeld dat het ecosysteem werkt is de ING. ING schiet zich in de voet wanneer zij aankondigen klant gegevens met derden te gaan delen, en komt door negatieve publiciteit en dreiging van handhaving terug op eerdere beslissingen. Het internationaal groot bedrijf heeft een monopolistische houding, de rekening van alles komt terecht bij het midden en klein bedrijf (MKB), die de negatieve gevolgen van de imperfecte markt dragen in termen van kosten. MKB Nederland geeft aan dat het knap lastig is voor het MKB om kredieten te kunnen krijgen. Transparantie betaalt zich niet af voor het MKB. De grote Gorilla is de overheid, per definitie monopolist. De overheid zit niet te wachten op perfecte markten. Maar de overheid moet niet ondernemen, dat moet de markt

doen. Er ligt wel degelijk een business case voor privacy innovaties. Het meldpunt datalekken zou een fantastische katalysator kunnen zijn. Maar ook de governance hoe, en dan met name (inzage in) aansprakelijkheden is een belangrijk aandachtspunt. Het gaat dan om bestuursaansprakelijkheid voor de bedrijfsvoering zelf, het verzekerd belang wordt breder waardoor rentekosten naar beneden gaan. Op het moment dat je deze wet- en regelgeving toepast gaan adviseurskosten naar beneden, meer voor de prijs van een, niet accountant én fiscalist, maar één overkoepelende financiële verantwoording voor meerdere doelen gebruiken. Het jaagt het proces van disintermediatie aan, het wordt transparanter en duidelijker. Dus ja, er is duidelijk een business case, waarbij de invloed van wet- en regelgeving, en dan zeker sancties en andere (mogelijke) kostenposten, een drijvende factor zijn. Evenwicht in de informatiemarkt is verstoord door asymmetrie, daar heb je wet en regelgeving voor nodig (met sancties en handhaving), die vervolgens de markt stimuleert tot innovatie.

3.4 Pitch Bart van der Sloot

In de pitch van Bart van der Sloot staat centraal dat het nooit de bedoeling is geweest om de bescherming van de consument centraal te stellen bij privacy. Bij privacy gaat het eigenlijk niet om een grondrecht maar om grondplicht: je mag als overheid niet zomaar in het privé leven van burgers zitten. Het is een waarborg tegen machtsmisbruik van de overheid. Dit is steeds meer tot een subjectief recht verworden van een persoon, die allerlei persoonlijke belangen probeert te beschermen, en hieruit is ook het gegevensbeschermingsrecht voortgekomen. Het idee hierbij was ook niet de bescherming van het individu, maar van gegevens. Gegevens waren niet privacygevoelig, veelal algemeen. Dan het individu centraal stellen is geen logische keuze geweest. Ten tweede werd een controlerecht zoals dat bij privacy wordt voorgestaan niet wenselijk geacht. Niet handig, want de overheid heeft gewoon heel veel gegevens nodig voor allerlei sociaal economische beleidsdoelen en dus ook bij gegevensbeschermingsrecht ging het om algemene principes, niet meer dan nodig, transparant, veilig. Niet het individu staat centraal, maar de integriteit van de data, de data set, het data systeem. Maar ook hier zie je een verschuiving waarbij steeds meer het individu centraal komt te staan, zoals ook blijkt uit de nieuwere rechten in de Privacy verordening. Steeds meer gegevens worden verzameld, steeds meer is persoonsgegeven. We zijn steeds meer met een begrip bezig dat alles kan omvatten, en om daarbij te zeggen dat het individu nog steeds centraal moet staan lijkt lastig, dus de focus op het individu en zijn belangen is niet langer houdbaar en niet legitiem. Zowel privacy als gegevensbeschermingsrecht dreigt een individueel klachtrecht te worden. Voor een groep is het moeilijk om op te komen voor privacy aangezien er allemaal individuele belangen centraal staan, die ook nog tegen andere individuele belangen worden afgewogen. Dit is niet houdbaar omdat je als individu niet weet wat er over je verzameld wordt. Het is niet realistisch om dit allemaal zelf te gaan beschermen. Terwijl het wel lijkt dat we daar naartoe gaan, naar rechten om individuele belangen te beschermen, maar ook steeds meer individuele verantwoordelijkheid om je eigen belangen te beschermen. Maar als je kijkt naar de NSA gaat het gewoon om de vraag of de overheid haar macht niet misbruikt, in plaats van dat ik als individu beschermd word. Ofwel, of mijn individuele belang nu afgewogen moet worden tegen het algemene belang van de overheid.

3.5 Pitch Ronald Leenes

Aangezien Ronald Leenes naast pitcher tevens optreedt als discussieleider begint zijn pitch met het aanbrengen van focus in de workshop. Er is reeds veel interessants gezegd, maar we lijken uit te waaieren (Snowden is al genoemd en ook het doel van dataprotectieregelgeving en privacybescherming). We hebben voor deze workshop een beperktere missie, die neerkomt op het volgende: We doen allemaal veel online, er wordt van alles van ons bewaard voor commerciële doeleinden, steeds vaker gaat het mis, en er wordt steeds agressiever gehandeld om gegevens van mij te achterhalen. Hoewel privacybescherming hier wellicht niet voor bedoeld was, lopen wij wel allerlei risico's die ontstaan door de zucht naar informatie. We hebben allerlei technieken die kunnen helpen bij het mitigeren van deze risico's. Ongeacht of dit de bedoeling is van privacy en privacy bescherming, kan het wel een rol spelen. We hebben een wettelijk kader, dat in principe hetzelfde doel heeft, vermindering van gegevens, meer transparantie, betere bescherming, etc. In de regelgeving ligt de plicht om privacy enhancing technologies te gebruiken, maar het gebeurt niet! Waarom niet? Het lijkt alsof we het reguleringskader niet hebben, niemand lijkt zich eraan te storen. Mensen kunnen bepaald gedrag vertonen als gevolg van een intrinsieke motivatie. In de wereld van gegevensverwerking lijkt geen intrinsieke motivatie te bestaan tot gegevensminimalisatie en privacy bescherming meer algemeen, het is meer andersom: 'data is the new oil'. Hoe gaan we dan extrinsieke factoren creëren? Dit kan positief met voordelen, of negatief, door met de stok te gaan slaan. Feit is dat het niet heel hard beweegt in de wereld van privacy enhancing technologies. Er zijn wel wat bewegingen, bijvoorbeeld in de wereld van cookies. Het aantal cookie walls gaat naar beneden en je ziet meer cookie management systemen ontstaan, er wordt in de nieuwere versies serieus getracht inzichtelijk te maken wat de consequenties van keuzes zijn. Maar waarom? Komt dit omdat de markt volwassen wordt? Of omdat privacy een differentiator wordt in de markt? Of zijn partijen aan het anticiperen op de Privacy verordening? In de markt van persoonsgegevens is er een inherent spanningsveld. Er zijn heel veel organisaties die gewoon zoveel mogelijk gegevens willen weten. We moeten niet aan kalkoenen vragen of we kerst moeten hebben. Dus wellicht moeten we het dan toch met regulering voor elkaar krijgen. Die lijkt momenteel niet te werken (er is immers al een bepaling in de Wbp die aanstuurt op PET's (art 13). Moet er dan meer of strengere wetgeving komen? Er waren nooit autogordels geweest als ze niet verplicht gesteld waren, en nu geloven we in auto gordels. De pitch wordt afgesloten met de stelling dat: de overheid regulerend op moet gaan treden met als risico dat je als overheid als te paternalistisch gezien wordt.

Annex 2: Workshopverslag

De regulering van privacy is in beweging. Momenteel wordt op Europees niveau gewerkt aan een Algemene Verordening Gegevensbescherming die de huidige Richtlijn Bescherming Persoonsgegevens uit 1995 zal gaan vervangen. Op nationaal niveau is deze Richtlijn omgezet in de Wet bescherming persoonsgegevens (Wbp). De Wbp biedt de kaders waarbinnen het toegestaan is om persoonsgegevens te verwerken. Tevens wordt er een aantal specifieke eisen gesteld waaraan voldaan moet zijn bij de verwerking van persoonsgegevens. De wettelijke vereisten zijn in de praktijk voor organisaties uitdagend genoeg. Voldoen aan de vereisten is in veel gevallen, met name voor kleine organisaties, al een lastige stap. Laat staan dat er ook nog pro-actief aan privacy-vriendelijke innovatie gewerkt wordt. Daar staat echter tegenover dat de regelgeving juist ook kan bijdragen aan innovatie. Het uitvinden van nieuwe technologische manieren om gegevens te beschermen of om aan de vereisten uit wet- en regelgeving te voldoen kan voor organisaties voordeel opleveren.

Hoewel er over het algemeen overeenstemming is over een aantal belangrijke aspecten van de innovatieve kracht van regulering, levert de hoofdvraag of het wettelijk kader voldoende prikkels biedt voor de uptake van privacy innovaties een divers beeld op. Enerzijds wordt aangegeven dat het wettelijk kader wel degelijk voldoende, met name negatieve, prikkels biedt die bedrijven ertoe zouden moeten bewegen privacy te verankeren in de bedrijfsvoering. Anderzijds klinkt sterk het geluid dat het wettelijk kader te complex is en dat vanuit andere hoeken handvatten en tools geboden zullen moeten worden om privacy innovaties daadwerkelijk in de maatschappij te doen landen. De bevindingen in dit hoofdstuk zijn gebaseerd op de discussie in een expertworkshop.

Niet de consument

Over het algemeen heerst de mening dat de verantwoordelijkheid voor privacy en gegevensbescherming niet volledig bij de consument gelegd kan worden. Consumenten zijn zich te weinig bewust van wat er allemaal speelt en hebben onvoldoende expertise om zich hiertegen met technische oplossingen te wapenen. Wat precies wel en niet van de consument verwachten mag worden is een lastig te beantwoorden vraag. Er lijkt een tendens gaande waarbij steeds meer van de consument verwacht wordt, maar gezien de asymmetrie tussen bedrijven en consumenten wat betreft informatie en kennis lijkt dit niet reëel.

Wet- en regelgeving: voor- en nadelen

Aangezien het niet aan de consument overgelaten kan worden, en velen van mening zijn (op een uitzondering daargelaten) dat ook de markt onvoldoende prikkels heeft om privacy innovaties op te pikken, richt het vizier zich op het regelgevend kader, waarin bepaald gedrag afgedwongen moet worden. Hier worden echter ook de nadelige kanten onderkend. Als de wet teveel verboden gaat bevatten, kunnen innovaties en kansen mogelijk in het gedrang komen door te restrictieve regels. Wanneer het gaat om big data initiatieven, dan is de privacy regelgeving vaak lastig om juist deze initiatieven te ontplooien. Het is immers een kenmerk van big data dat op voorhand niet altijd bekend is waarnaar precies gezicht wordt, maar dat pas later verbanden gelegd worden. De vraag

die dan opkomt is hoe zich dit verhoudt tot bijvoorbeeld het principe van doelbinding in privacywetgeving. Wetgeving moet niet een compleet chilling effect hebben op waardevolle nieuwe technologieën die veel voordelen met zich kunnen brengen. De uitdaging is dus om binnen die wetgeving een level playing field te creëren waarbij privacy en innovatie beiden bescherming en ruimte krijgen?

Een ander probleem van wet- en regelgeving is dat deze altijd achterloopt op actuele technologische ontwikkelingen. Het is moeilijk voor de overheid om steeds op elke ontwikkeling in te springen, wellicht zelfs niet realistisch. Ook kan er te vroeg worden ingegrepen. Het Collingridge dilemma ligt hier op de loer: het is moeilijk te voorspellen wat een technologie gaat doen voordat deze voldoende ontwikkeld is. Aan de andere kant is het vaak moeilijk om nog in te grijpen als een technologie al ver ontwikkeld is. Weer een ander risico is gelegen in de afweging tussen techniekneutraliteit en helderheid en kenbaarheid van wet- en regelgeving. Te open normen creëren onduidelijkheid en ruimte voor verschillende interpretaties, terwijl te gedetailleerde wetgeving al snel niet techniekneutraal zal zijn. Hier zal een middenweg in gevonden moeten worden.

Technologische standaarden kunnen een oplossing bieden, maar standaarden kunnen doorschieten in bescherming. De ideeën van wat privacy precies is zijn divers, waardoor een strikte en homogene bescherming van consumenten ook als paternalistisch opgevat kan worden. Er zullen immers ook consumenten zijn die helemaal geen bescherming willen, maar de vrijheid voorop stellen om te doen en laten met hun gegevens wat ze willen. Dus standaarden zouden vanuit het algemeen belang opgesteld moeten worden. Goede standaarden zullen in dat geval ook de uiteenlopende belangen van individuele consumenten afzonderlijk behartigen. Het gaat om het voorkomen van machtsmisbruik, door het organiseren van tegenmacht.

Intermediairs?

Naast de overheid zouden ook andere partijen zoals belangenorganisaties zoals bijvoorbeeld de consumentenbond, een rol kunnen spelen in het vergroten van het online vertrouwen van consumenten en in het zorgvuldig gebruik van data door dienstverleners. Een vergelijkbaar voorbeeld is Bovag in de autobranche, die bepaalde garanties geeft die consumenten vertrouwen bieden, of het gebruik van keurmerken, een redelijk gangbaar gebruik in de e-commerce sector. Het is nog een open vraag of, en zo ja hoe, dit gerealiseerd kan worden voor het privacydomein? Binnen dit domein bestaan al Privacy officers en functionarissen gegevensbescherming, maar wellicht kunnen meer onafhankelijke organisaties wel degelijk meerwaarde bieden.

Naast organisaties wordt ook gewezen op mechanismen, zoals bijvoorbeeld het systeem van TRIPadvisor. Met behulp van smileys (☺) worden adviezen gevisualiseerd om zo consumenten te helpen bij het maken van bepaalde online keuzes. De overheid lijkt positief te staan tegenover zelfreguleringsinitiatieven. Wetgeving wordt gezien als soort van ultimum remedium als zelfregulering onvoldoende bijdraagt aan de landing van privacy innovaties in de praktijk. Het blijkt echter ook dat pure zelfregulering, zonder sturing vanuit de overheid vaak niet de beoogde bescherming van consumenten oplevert.

Negatieve prikkels

Bij negatieve prikkels gaat het met name om sancties, of de dreiging daarvan. Een vraag die hiermee nauw verbonden is, is of de toezichthouder dan ook meer capaciteit nodig heeft om meer te gaan handhaven. Zonder deze daadwerkelijke handhaving hebben hogere boetebevoegdheden immers weinig zin en ook slechts beperkt preventief effect. Een boete zal ook in verhouding staan tot de omzet van een bedrijf. Een MKB bedrijf met een jaaromzet van 60.000 euro zal geen boete van 450.000 euro opgelegd krijgen, maar een lagere boete die in verhouding staat tot de omzet. Daarmee blijft toch een risico-afweging mogelijk, mede afhankelijk van de handhaving in de praktijk. In de discussie komt duidelijk naar voren dat niet alleen vanuit het CBP dreiging van sancties komt. Er zijn 40.000 accountants die naleving van de wet gaan controleren. Zij controleren op een fout van materieel belang bij de controle van de jaarrekeningen van bedrijven (omdat de sanctie hoog genoeg is). Als accountants de jaarrekening controleren, moeten zij ook financiën opnemen voor de mogelijke negatieve gevolgen van bijvoorbeeld een datalek. Dat leidt ertoe dat bedrijven extra reserveringen moeten maken voor eventuele schades waar ze op afgerekend kunnen worden. Accountants gaan dus actief toezien op het handelen van het bestuur inzake gegevensbescherming en privacy, onder andere via de jaarrekeningsplicht. De hogere boete zoals voorgesteld in de aankomende Verordening biedt een duidelijke prikkel die deze vorm van controle door accountants versterkt.

In het verlengde hiervan kunnen marktpartijen zich meer privacy bewust opstellen. Een commercieel bedrijf reageert op financiële gevolgen met als gevolg dat sancties een sturend karakter hebben. Sommige partijen hebben het idee dat bedrijven al sinds 1995 worden geholpen met de implementatie van dataprotectie. Daarom heerst soms de opvatting dat er nu wel genoeg geholpen is en dat bedrijven het zelf moeten kunnen. Er is een nieuw eco-systeem, waarbij partijen in kunnen springen op onwetendheid en de dreiging van consequenties van niet voldoen aan wet- en regelgeving. Of dat daadwerkelijk zo is, daarover lopen de meningen uiteen. Dat niet alles geheel duidelijk of evident is lijkt te kloppen. Het bewuste misbruik van die situatie is echter onvoldoende onderbouwd om een stellige uitspraak over te doen.

Kritische geluiden ten aanzien van de daadwerkelijke effecten van de inzet van accountants als controle op privacy compliance zijn er ook, aangezien de verplichtingen rondom de jaarrekening nu reeds bestaan. De cookiewetgeving kent al een boete van 450.000 euro, terwijl de effecten daarvan nog niet zichtbaar zijn in de jaarrekeningen. Accountants worden in de opleiding meer en meer gewezen op de verplichtingen rond fouten van materieel belang (en de rol van dataprotectie daarin). Het is mogelijk accountants aansprakelijk te stellen voor gebreken in de controle van de jaarrekeningen op dit vlak, dus de praktijk van dataprotectie handhaving via de band van accountants zou zich moeten gaan ontwikkelen. Ook een organisatie zoals de AFM zal hier op toe gaan zien, hetgeen inhoudt dat meerdere toezichthouders in zullen staan voor de borging van privacy belangen. De Nederlandse Mededingingsautoriteit[15] heeft al een boete uitgedeeld voor een niet geoorloofde voeging van databestanden tussen bedrijven.

Een ander kritisch geluid betreft het feit dat de weg via de accountant wel erg dicht raakt aan compliance: het voorkomen van schade door wettelijke aansprakelijkheden. Het is jammer om daarmee de prikkel weg te nemen dat privacy ook een kans kan zijn. Een dergelijke ontwikkeling zie

[15] NMa, tegenwoordig onderdeel van de Autoriteit Consument en Markt (ACM).

je ook wel binnen bedrijven zelf, bijvoorbeeld door het overleg met privacy officers. Zo zijn er al enkele bedrijven waar de privacy officers niet alleen denken vanuit compliance, maar ook vanuit innovatie. De NS is hier een mooi voorbeeld van.

Positieve prikkels

Naast negatieve prikkels, die gelegen zijn in de sanctie-sfeer, kunnen ook positieve prikkels bijdragen aan de adoptie van privacy innovaties. Ook deze kunnen gestimuleerd worden middels wetgeving. Een mogelijkheid is bijvoorbeeld om, wanneer een bedrijf bewust omgaat met privacy enhancing technologies (PETs), toe te staan dat meer gedaan wordt met de verzamelde (persoons)gegevens. Dit zou een positieve prikkel tot de invoering van PETs kunnen bieden, en sluit aan bij uitgangspunten in de voorgestelde Verordening dat meer zou mogen met geanonimiseerde of gepseudonimiseerde gegevens. Bedrijven die bewust omgaan met privacy en gegevensbescherming zouden hiervoor van het CBP een pluim moeten krijgen, of anderszins een positieve beloning kunnen krijgen.

Accountability kan naast als een negatieve, ook als een positieve incentive gezien worden, waarbij bedrijven zelf proactief kunnen etaleren wat zij allemaal doen en hierop kunnen scoren. Dit zou ook kunnen door zogenaamde 'Transparency Reports'. Dergelijke rapporten kunnen een positieve prikkel vormen voor de implementatie van privacy innovaties, met name wanneer het om vergelijkende rapporten gaat. In de VS hebben deze rapporten, die een rating geven aan hoe je voldoet aan bepaalde overheidsverzoeken en plichten, grote invloed.

Het is van belang te beseffen dat niet alle PETs gelijk zijn. Dataminimalisatie is een beleidsmatige vraag voor het management (kunnen we onze doelen bereiken met minder data). Beveiligingsmaatregelen zijn conceptueel anders en vergen andere initiatieven. Dit is een gedeeld belang tussen consument en bedrijf. Het ene raakt de bedrijfsvoering, en het andere is meer de operationele sfeer, en dit verschil vergt conceptueel een andere benadering.

Helpende hand bedrijven: ondersteunende toezichthouder

Bij bedrijven is privacy lang niet altijd een zaak van onwil, maar vaak een zaak van onwetendheid en onkunde. Bedrijven weten niet wat ze moeten doen aan beveiliging. Dit zou verholpen kunnen worden met een minimale set van voorwaarden. Ook een meer substantiële rol voor de Privacy Officer (PO) – nu vaak een functie die naast een andere functie erbij gedaan moet worden –, zou verbetering kunnen brengen. Ook vanuit het oogpunt dat de PO niet altijd volledig onafhankelijk is en dus niet altijd ongehinderd privacybelangen kan verdedigen ten opzichte van een bedrijfsvoering, is verbetering mogelijk.

Het CBP zou veel meer moeten doen aan voorlichting en het bieden van een handvat (in zekere zin een terugkeer naar eerder beleid van het College). Er wordt een behoefte aan een minimale set voorwaarden gesignaleerd waaraan bedrijven gewoon moeten voldoen, en waarop het CBP niet alleen handhaaft, maar ook voorlichting geeft. Een simpel voorbeeld van wat opgenomen zou kunnen worden in zo'n minimale set voorwaarden, is dat communicatie met gebruikers/klanten (bijvoorbeeld via email) versleuteld moet plaatsvinden. Dat hoeft niet heel veel meer te kosten,

maar levert direct iets op, en het biedt ook de juiste en duidelijke handvatten waar een bedrijf aan moet voldoen. Denk bijvoorbeeld aan een minimumlijst van maatregelen voor een bedrijf wat gedaan moet worden, met name beveiligingsmaatregelen. Hierbij kunnen op eenvoudige wijze handvatten gegeven worden om bedrijven concreet verder te helpen. Bedrijven zijn niet altijd in staat om zelf het juridisch kader correct toe te passen, zij moeten geholpen worden met uitleg. Hierover lijkt men het eens te zijn. Of deze uitleg van de overheid of van de markt moet komen, daar lijken de meningen echter over verdeeld te zijn.

In de discussie klinkt de behoefte door van een actieve toezichthouder, die actief publiceert en die actief het bedrijfsleven informeert wanneer en hoe bedrijven bepaalde data protectieverplichtingen hebben. Hoewel het CBP geen set van minimum voorwaarden heeft, is er wel een praktijk opgebouwd van richtlijnen (zoals de Richtsnoeren beveiliging persoonsgegevens[16] die het beleidskader gedetailleerd invullen). Probleem is alleen dat bedrijven de weg naar het CBP niet weten te vinden, of als ze hem vinden nul op het rekest krijgen. Zelf uitzoeken waaraan voldaan moet worden is dan vaak te lastig of onhandig en wordt dan gewoonweg niet gedaan. Er zijn echter wel partijen die dienstverlening hierin aanbieden, maar voor met name kleine bedrijven kan dat een relatief grote financiële investering betekenen die niet wordt gedaan zolang de urgentie niet heel duidelijk aanwezig is. Het bieden van een praktische minimum voorwaarden set zou zelfs uitgebreid kunnen worden met het actief voorzien in bruikbare technische tools. Implementatie en naleving zouden ook hier afgedwongen kunnen worden door sancties. Vooralsnog is de markt niet erg geschrokken van de tot nu toe genomen maatregelen van het CBP, en dan handelt de markt er ook niet naar.

Het spreekt overigens voor zich dat er geen praktijk moet ontstaan waarin het CBP zichzelf goedkeurt. Voorafgaand een innovatie goedkeuren zonder voorbehoud is niet mogelijk, omdat dat conflicteert met de rol als toezichthouder. Meer informeel meedenken kan echter wel bijdragen aan een privacyvriendelijker innovatielandschap.

Een minimum set aan voorwaarden kan ook positieve effecten voor bedrijven hebben doordat het kan bijdragen aan kostenverlaging, en een middel kan zijn dat bijdraagt aan het uitleggen aan de consument dat er deugdelijk met privacy en gegevensbescherming wordt omgegaan. Een ander voordeel van praktische harmonisatie is dat het voor alle bedrijven gelijk is. Een voorbeeld waar het lijkt te werken is het standaard herroepingsformulier uit het e-commerce kader. Hiermee zijn er geen extra kosten voor het bedrijf, het bedrijf weet dat ze het goed doen, en de consument kan erop vertrouwen. Overigens kan een dergelijke set voorwaarden ook aangeleverd worden door standaardisatieorganen, zoals bijvoorbeeld ook met de ISO-normen gebeurt.

De adviezen geproduceerd via de bestaande kanalen zoals het CBP en de Art.29 werkgroep zijn voor niet juristen niet goed te behappen. Als het CBP niet in staat is meer handzame sturing te geven, onder meer door capaciteitsgebrek, rijst de vraag wie dat wel moet doen.

[16] Zie: http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.

Privacy als keus/marktdifferentiator

Er kan een positief effect ontstaan wanneer bedrijven aan consumenten kunnen uitleggen wat ze doen om privacy te beschermen. Bedrijven zitten niet te wachten op een datalek, dus zij willen het zeker goed doen. Maar verder dan alleen een beveiligingstechnische benadering gaat de keuze voor privacy als marktdifferentiator. Een fundamentele uitleg van actieve stappen om privacy beter dan gemiddeld te beschermen kan een concurrentievoordeel opleveren. Dat betekent wel dat een bedrijf het ook goed moet kunnen uitleggen; goede communicatie is essentieel. Er is een brede set aan design patterns voor data processing, data transfer, data management etc. die gebruikt kunnen worden in het ontwerp en communicatie over de resulterende infrastructuur.

Echt laten zien hoe een bedrijf de privacy beschermt is vaak echter lastig. Veel zit in de techniek die de consument niet ziet. Transparantierapporten en PIA's worden niet door consumenten gelezen, maar zijn wel een instrument dat door openbaarheid vertrouwen kan wekken. Een tegenwerping bij transparantierapporten is dat dit misschien waardevolle informatie voor hackers oplevert. Dit risico werd in de discussie weergesproken.

Er bestaat wel een zeker spanningsveld tussen transparantie en vertrouwen. Een voorbeeld dat dit illustreert betreft bodyscanners op luchthavens. De eerste generatie toonde zeer aanschouwelijk het menselijk lichaam van de passagier. De tweede versie werkte met een meer geabstraheerde weergave (stick figure). Na discussie is toch gekozen voor de eerste, omdat de technologie daar transparanter is, het is beter zichtbaar wat die technologie doet. Misschien dat het dus toch wenselijker is dat een 'instantie' privacy praktijken screent en bijhoudt. Transparantierapporten kunnen daar bij helpen.

Link met milieu

Er is een analogiemogelijk tussen privacy- en milieuwetgeving. Op de ene plaats is er vervuiling, maar de slachtoffers zitten ergens anders. Ook met de verwerking van persoonsgegevens kunnen elders slachtoffers gecreëerd worden. De kreet 'een beter milieu begint bij jezelf' is niet zo eerlijk. Dat geldt ook voor privacy. Gepleit wordt voor een fairtech trademark dat verder gaat dan enkel privacybelangen. Ook bij milieu zijn er hele duidelijke wettelijke normen gekomen, dus voor privacy zou dat ook moeten kunnen. En in de milieucontext zie je wel bedrijven die groen als selling point gebruiken, maar vaak alleen commercieel en niet zozeer vanuit ideologie of overtuiging. Eenzelfde verschijnsel zie je bij privacy, bijvoorbeeld bij 'privacywashing' (net zoals 'greenwashing') waar de illusie wordt gewekt privacyvriendelijk te zijn, terwijl dat in de praktijk niet het geval is.

Het is onwenselijk om de discussie over grondrechten (zoals privacy) volledig te framen in een totaal economische setting die gaat over consumptiegroei. De discussie moet veel verder gaan dan de puur monetaire belangen. Dat kan dus mogelijk ook betekenen dat sommige businessmodellen illegaal verklaard zullen worden.

Checks and balances

De ontwikkelingen in de privacywetgeving worden door veel experts positief bestempeld. Dataprotectiewetgeving hindert de privacy innovatie niet, maar stimuleert deze juist. Het geeft

enorme voordelen aan bedrijven en consumenten wanneer privacy innovaties stevig worden doorgezet.

Het toezichtarrangement moet adequaat georganiseerd worden. Vrijheid staat bovenaan en het vertrouwen in informatie en transacties is essentieel. De macro- en meso-economische voordelen die te behalen zijn vormen in die zin een soort restproduct, maar wel van grote waarde. Er zijn voldoende checks and balances beschikbaar om dit toezicht adequaat te organiseren.

Tussenconclusie

Als individu loop je concrete risico's doordat heel veel bedrijven gegevens verzamelen, soms zonder legitieme grondslag, en soms zonder aan de wettelijke vereisten omtrent bewaartermijnen en beveiliging etc. te voldoen. Wetgeving alleen biedt onvoldoende prikkels om privacybescherming af te dwingen. Toch is er wel wat beweging in de wereld van het gebruik van PETs. De vraag is hoe dit komt? Mogelijkheden zijn:

1. De markt wordt volwassen
2. Privacy wordt gezien als differentiator
3. Anticipatie op de voorgestelde Algemene Verordening Gegevensbescherming

Het huidige wettelijke kader is te ingewikkeld voor consumenten en bedrijven. De verantwoordelijkheid voor bescherming van privacy en gegevensbescherming door gebruik te maken van privacy-innovaties kan niet bij de consument gelegd worden. Zelfs met een toenemend consumentenbewustzijn is er onvoldoende zicht op de risico's en zijn consumenten onvoldoende kundig om (technische) innovatieve maatregelen te implementeren. Ook kunnen zij de markt niet significant beïnvloeden. Er komen echter steeds meer verantwoordelijkheden te liggen bij de consument, die daar niet kunnen liggen.

Er blijft een inherent spanningsveld om oplossingen in de wetgeving te zoeken. Immers, als het huidige reguleringskader, waar veel reeds in is opgenomen, niet werkt, waarom zou een nog uitgebreider kader dan wel werken? Bij bedrijven zal er alleen sprake zijn van uptake als er positieve dan wel negatieve prikkels geboden worden die het bedrijfsbelang van implementatie van dataprotectiemaatregelen duidelijk maken. Hier kan wetgeving wel een rol in spelen aangezien de wet positieve en negatieve prikkels kan genereren: controle en handhaving, hogere boetes, keurmerken, subsidies, etc. Hoewel bedrijven privacy steeds meer als markt zien, moet hierbij worden opgemerkt dat wat gepretendeerd wordt met betrekking tot privacy, lang niet altijd een correcte weergave van de werkelijkheid is. Gepoogd wordt privacy als selling point te benutten, gebruik makend van de onwetendheid van de consument over de daadwerkelijke invulling van de privacy standaard. Vanuit dit perspectief kan geopperd worden dat de adoptie van privacy innovaties niet alleen aan bedrijven kan worden overgelaten.

Aan de andere kant kan beargumenteerd worden dat juist door de toename in negatieve prikkels (meer controle, meer audits, meer verantwoording op bijvoorbeeld jaarrekeningen, hogere boetes) en de positieve prikkels die hiermee samenhangen in de zin van kostenbesparing, efficiëntie en

privacy als selling point, de markt het wel degelijk op zal pakken. Bedrijven moeten wel, omdat het huidige en toekomstige juridische kader dit afdwingt.

Meer positief kunnen keurmerken, of een pluim van het CBP genoemd worden als een stimulans voor de uptake van privacy innovaties. Simpele inzichtelijke online tools, zoals bijvoorbeeld ☺ en ☹ zijn begrijpelijk voor burgers en vormen een middel voor bedrijven om zich te profileren. Hierbij geldt dan wel dat een toezichthoudend orgaan, een belangen- of brancheverenigingen (partijen als het CBP, Consumentenbond) toezicht en controle uit moeten oefenen en het ontnemen van het keurmerk en eventueel andere sancties tot de mogelijkheden moeten behoren. Hierbij geldt bovendien dat dergelijke organisaties bedrijven zullen moeten helpen met duidelijke handvatten en tools. Een andere mogelijke prikkel is gelegen in zogenaamde Transparency Reports, een in de VS bekend fenomeen. Het zijn vergelijkende rapporten (De Electronic Frontier Foundation (EFF) geeft ratings aan bedrijven over hoe ze omgaan met gegevens). Uit de discussie volgt dat het regulerend kader niet alleen hekken moet zetten, maar juist ook moet stimuleren.

Bij het aanbieden en ontwikkelen van privacy innovaties moet rekening gehouden worden met het feit dat sommige wettelijke concepten in de praktijk simpelweg niet werken, zoals bijvoorbeeld geïnformeerde toestemming, hetgeen veel te breed en onoverzichtelijk is. Een dergelijk vereiste zal dan ook op een wijze vormgegeven moeten worden waarin het doel van de wet mogelijk wel tot zijn recht komt, zoals bijvoorbeeld het aanbieden van vormen van layered consent. Ook gebruikersvriendelijkheid, voorlichting en assistentie zijn belangrijke voorwaarden om privacy innovaties bij consumenten te laten landen. Consumenten hebben online vertrouwen nodig. Als de gebruiker niet beschermd wordt, wat doet dat dan met ie gebruiker? Is het de privacy zelf die innovatie belemmert, of is het het ontbreken van vertrouwen dat privacy belemmert?

Hoewel het recht op privacy en gegevensbescherming en de noodzaak van de acceptatie en implementatie van privacy innovaties om de bescherming van deze rechten beter te garanderen voorop staan, moet er ook voor gewaakt worden dat de overheid zich niet teveel mengt in de markt.

Annex 3: Desk Research

Actieplan Privacy

Een inventarisatie van Best Practices & Best Technologies

Datum:	3 juli 2013
Auteurs:	Colette Cuijpers, Just Eijkman, Marc van Lieshout, Arnold Roosendaal, Bas van Schoonhoven, Anne Fleur van Veenstra.
Opdracht:	Deze opdracht is uitgevoerd door het Privacy & Identity Lab in opdracht van het Ministerie van Economische Zaken. Deze opdracht is uitgevoerd onder de in de offerte genoemde voorwaarden. Aanbiedingsbrief: 2012-MII-344-FvA-NvB Offertenummer: 900797
Penvoerder:	Penvoerder voor deze opdracht namens het Privacy & Identity Lab: TNO.

Dit rapport is geschreven door het Privacy & Identity Lab en vertegenwoordigt niet het standpunt van de Minister van EZ. De Radboud Universiteit, TNO, Tilburg University en SIDN, het bedrijf achter.nl, werken gezamenlijk aan betere oplossingen voor het beheren van online privacy en elektronische identiteiten. Daartoe hebben ze het Privacy & Identity Lab opgericht, een expertisecentrum waarin ze bestaand onderzoek bundelen en nieuw onderzoek opzetten. Het samenwerkingsverband is uniek, omdat het de technische, juridische en socio-economische aspecten van privacy en identiteit integraal onderzoekt.

Inhoudsopgave

1 Inleiding

De aandacht voor privacybescherming van burgers en consumenten is onverminderd hoog. In de Monitor ICT, Veiligheid en Vertrouwen 2012 door TNO[17] is bezorgdheid om privacy de meest genoemde reden voor consumenten om van het gebruik van een dienst op internet af te zien. Zoals het in de recente kabinetsbrief aan de Tweede Kamer over e-Privacy gesteld wordt: een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer draagt bij aan het digitale vertrouwen van betrokkenen en daarmee aan de groei van digitale diensten.[18]

Privacy biedt kansen voor innovatie, en vormt soms een barrière voor internetdiensten. Er is en wordt veel technologie ontwikkeld die uitzicht biedt op slimme privacy-vriendelijke oplossingen in bedrijfsprocessen. Kansen liggen er niet alleen in het toepassen van deze oplossingen waarmee risico's vermeden worden en de zorg om privacy als een *unique selling point* kan gelden, maar ook in het verder ontwikkelen en vermarkten van deze oplossingen. Een voorwaarde voor het grijpen van deze kansen is dat er voldoende kennis over aanwezig moet zijn bij bedrijfsleven en publieke organisaties, en inzicht in de mogelijkheden die de oplossingen kunnen bieden. Juist deze kennis en dit inzicht is niet altijd aanwezig.

Het Actieplan Privacy heeft als doelstelling dit hiaat op te vullen, en daarmee de belangrijke dienstensector in Nederland tot privacy-vriendelijke innovatie te stimuleren zodat ze zich daarmee op het gebied van privacy een vooraanstaande positie kan verschaffen.

Dit rapport is het resultaat van de eerste activiteit van het actieplan: een literatuurstudie naar technologieën en praktijken die veelbelovend zijn, zogenaamde *best technologies* en *best practices*. Een *best technology* of *best practice*: (1) is effectief in het beschermen van privacy; (2) heeft zich bewezen in proof-of-concepts, pilots of de praktijk; en (3) biedt bedrijven een kans om te innoveren.

De literatuurstudie heeft als primair doel om te komen tot een brede inventarisatie van *best technologies* en *best practices*. Tijdens het werken aan deze inventarisatie bleek al snel dat de gevonden oplossingen zich op veel verschillende niveaus van abstractie bevinden, en dat geïsoleerde oplossingen niet tot effectieve privacybescherming leiden. Om een toegankelijke ingang te bieden tot de geïnventariseerde *best technologies* en *best practices* zijn ze daarom gegroepeerd in 'combinaties' die in samenhang een effectieve oplossing bieden.

De volgende stap in het Actieplan is het verrijken en verfijnen van de inventarisatie door consultatie van bedrijven en organisaties die ervaring hebben met het invoeren van privacy-vriendelijke oplossingen in bedrijfsprocessen, daar voor open staan of zelf privacy-vriendelijke oplossingen ontwikkelen. Het uiteindelijke doel daarbij is om een aantal kansrijke *best innovations* (mogelijk combinaties van *best technologies* en *best practices*) een stap verder te brengen en uit te diepen door coalities te vormen rond deze innovaties in samenwerking met belangrijke stakeholders als ECP, VNO/NCW en ICT Office.

[17] TNO, 2012, Monitor ICT, Veiligheid en Vertrouwen.

[18] Ministerie van Economische Zaken, Brief Kabinetsvisie op e-privacy: op weg naar gerechtvaardigd vertrouwen, 24 mei 2013

2 Combinaties van *best technologies* en *best practices*

Oplossingen voor privacybescherming die in de literatuur naar voren komen zijn er in alle soorten en maten: concrete technologieën, concepten die richting geven bij het ontwerp van systemen, richtlijnen en principes, handvaten om organisatorische processen in te richten, en veel meer. Deze grote verscheidenheid van *best practices* en *best technologies* maakt het overzichtelijk in kaart brengen van de oplossingen een uitdaging.

We presenteren de gevonden *best technologies* en *best practices* hier in combinaties die in samenhang een oplossing kunnen bieden voor een bepaald probleem rond privacybescherming. Bij het opstellen van de combinaties is gezocht naar een pragmatische aanpak; iedere ordening omvat een zekere willekeur. We hebben er voor gekozen de combinaties globaal te ordenen op drie niveaus: oplossingen die zich richten op het verbeteren van netwerken, diensten en de positie van de persoon van wie gegevens verwerkt worden: het data subject.

Oplossingen voor het verbeteren van diensten

Binnen de oplossingen die zich richten op het verbeteren van diensten maken we onderscheid tussen die *best technologies* en *best practices* die zich richten op het ontwerpen van een informatiesysteem en die zich richten op het inrichten van de organisatie:

(1) Ontwerpen voor privacy
Welke oplossingen kan een ontwerper gebruiken bij het ontwerpen van een dienst waarin persoonsgegevens verwerkt worden?
(2) Inrichten van processen en organisatie
Welke oplossingen helpen management om een organisatie en de processen in die organisatie zodanig in te richten dat privacybescherming versterkt wordt?

Oplossingen voor het verbeteren van netwerken van organisaties en individuen

De oplossingen die zich richten op het verbeteren van privacybescherming op het niveau van netwerken van organisaties en individuen scharen we onder de noemer “vertrouwensnetwerken”:

(3) Vertrouwensnetwerken
Welke oplossingen stellen groepen van stakeholders in staat om gezamenlijk tot een vertrouwenwekkende bescherming van persoonsgegevens te komen?

Oplossingen voor het versterken van de positie van het data subject

Binnen de oplossingen die zich richten op het verbeteren van de positie van het data subject maken we onderscheid tussen die *best technologies* en *best practices* die zich richten op het voorlichten van gebruikers en ze in een dienst een goede keuze te bieden wat betreft de wijze waarop met zijn of haar persoonsgegevens omgegaan wordt, en hulpmiddelen die een individu in staat stellen zelf zorg te dragen voor zijn of haar privacy:

(4) Geïnformeerde instemming
Welke oplossingen kan een ontwerper gebruiken om gebruikers van een dienst goed te informeren over de wijze waarop met persoonsgegevens omgegaan wordt en ze daarin een betekenisvolle keuze te bieden?

(5) Zelfredzaamheid in privacy
Welke (eventueel betaalde) oplossingen stellen een burger of consument in staat om zelfstandig zijn of haar privacy te beschermen?

Bij elke combinatie omschrijven we kort het probleem en de doelgroep. Het belangrijkste deel van de combinatie omschrijving bestaat uit een lijst van *best technologies* en *best practices* die we onder de combinatie scharen, en die, vaak in samenhang, een oplossing kunnen bieden. De *best technologies* en *best practices* worden omschreven in een *fact sheet*. Voor elke *best technology* en *best practice* (hieronder samen omschreven als "oplossing") omschrijven we het volgende:

- **Waartoe** dient de oplossing?
  Bijvoorbeeld: verantwoording, afscherming
- **Wanneer** is de oplossing van belang in het bedrijfsproces?
  Bijvoorbeeld: vooraf, tijdens of na afloop van de verwerking
- **Waarop** heeft de oplossing betrekking in het bedrijfsproces?
  Bijvoorbeeld: verzamelen, verwerken, delen van persoonsgegevens
- **Wie** is verantwoordelijk binnen of uiten de organisatie voor het realiseren van de oplossing?
  Bijvoorbeeld: directie, management, IT-verantwoordelijke, gebruiker of externe partij
- **Hoe** werkt de oplossing?

Daarnaast geven we waar mogelijk een voorbeeld uit de praktijk en verwijzingen naar aanvullende informatie.

De beschreven *best technologies* en *best practices* variëren van het zich uitgebreid bewezen hebben in de praktijk tot nog vrij theoretische en nog vrijwel niet toegepaste oplossingen. In de consultatierondes die op deze inventarisatie volgen is één van de doelen het vinden van die *best technologies* en *best practices* die potentieel hebben tot uitvoerbare innovatie.

2.1 Ontwerpen voor privacy

Welke oplossingen kan een ontwerper gebruiken bij het ontwerpen van een dienst waarin persoonsgegevens verwerkt worden?

Een van de meest besproken concepten als het om privacy en informatietechnologie gaat is *Privacy by Design*: het al bij het vroegste ontwerp van een informatiesysteem rekening houden met privacy. Ontwerpen voor privacy heeft zowel een organisatorische als een technologische kant. Oplossingen voor het ondersteunen van het ontwerpproces zijn er in verschillende vormen zoals algemene *Privacy Design Strategies* en *Privacy Design Patterns*, het toepassen van anonimisering en pseudonimisering, aandacht voor de user interface aspecten van privacy en het hanteren van standaarden voor informatiebeveiliging.

2.1.1 Privacy by Design

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Bieden van een omvattende benadering voor de integratie van privacybescherming in diensten en systemen.	*Privacy by Design heeft betrekking op de gehele levenscyclus van een gegevensverwerkende dienst of systeem. Het poogt in de ontwerpfase privacybescherming een plaats te geven.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Privacy by Design heeft betrekking op het gehele gegevensverwerkende proces, en heeft oog voor technische en organisatorische elementen.	*Privacy by Design heeft steun nodig van directie en management. De IT-verantwoordelijke en functionaris gegevensbescherming gaan er mee aan de slag.*

Privacy by Design is een ontwerpbenadering en niet zozeer een concrete praktijk of technologie. Een bedrijf, organisatie of projectteam doet aan *Privacy by Design* als bescherming van de privacy al bij het vroegste ontwerp van een systeem wordt meegenomen, en deze aandacht voor privacy doorgaat gedurende de gehele levenscyclus van het systeem. Dit vormt een contrast met een aanpak waarbij men pas nadat een dienst of systeem operationeel is of pas nadat er incidenten optreden over privacy wordt nagedacht. Het achteraf toevoegen van privacybescherming aan een systeem of dienst is vaak lastiger en duurder dan wanneer dit gelijk in het ontwerpproces wordt meegenomen. De ontwerpbenadering van *Privacy by Design* gaat niet alleen over het gebruik van technologie, maar ook over de wijze waarop de organisatie wordt ingericht.[19]

De Canadese toezichthouder Ann Cavoukian heeft veel betekend in uitwerking en verspreiding van de gedachten achter *Privacy by* Design.[20] Inmiddels is de term wereldwijd gemeengoed geworden, en noemt ook het College Bescherming Persoonsgegevens *Privacy by Design* als een uitgangspunt om tot een passende beveiliging van persoonsgegevens te komen.[21] Een eenduidige nadere uitwerking van wat *Privacy by Design* in de praktijk betekent, is er niet. Wel zijn er inmiddels veel

[19] TNO, 2012, Stimulerende en remmende factoren van Privacy by Design in Nederland http://www.tno.nl/content.cfm?context=thema&content=prop_publicatie&laag1=897&laag2=919&laag3=114&item_id=878

[20] Cavoukian, 2009, Privacy by Design http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

[21] CBP, 2013, Richtsnoeren beveiliging persoonsgegevens http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx

best practices en *best technologies* beschikbaar waarmee een organisatie aan de *Privacy by Design* ontwerpbenadering invulling kan geven.

Voor het volgen van een *Privacy by Design* aanpak worden verschillende redenen aangevoerd: het willen voldoen aan de wetgeving, het vermijden van een boete en imagoschade, het aantonen dat de organisatie privacy serieus neemt, of dat het recht op privacy belangrijk gevonden wordt. Er wordt door verschillende instellingen gewerkt aan de verdere uitwerking van *Privacy by Design*, gericht op een concrete toepasbarheid in de praktijk. Eén van de problemen die overwonnen moet worden is de invoering van *Privacy by design* in al bestaande systemen (het *legacy*probleem). De aandacht voor *Privacy by Design* is dankzij een toenemend privacybewustzijn bij bedrijven en consumenten en strikter wordende regelgeving wel aan het toenemen.

Voorbeeld: Privacy by Design in Smart Grids

Een van de voorbeelden die Cavoukian gebruikt om het *Privacy by Design* concept te promoten is een *Smart Grids* case in Ontario, Canada waarin bij de introductie van een smart grids infrastructuur nagedacht is over hoe privacy goed te beschermen, vanaf het vroegste begin. Enkele maatregelen die als gevolg van het hanteren van een *Privacy by Design* aanpak hier genomen zijn, zijn het scheiden van domeinen (bijvoorbeeld klantendomein en grid-domein) en waar mogelijk het samenvoegen van verbruiksgegevens .

Meer lezen over deze case:
http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf

Andere cases worden ook genoemd op de *Privacy by Design* website:
http://www.privacybydesign.ca/

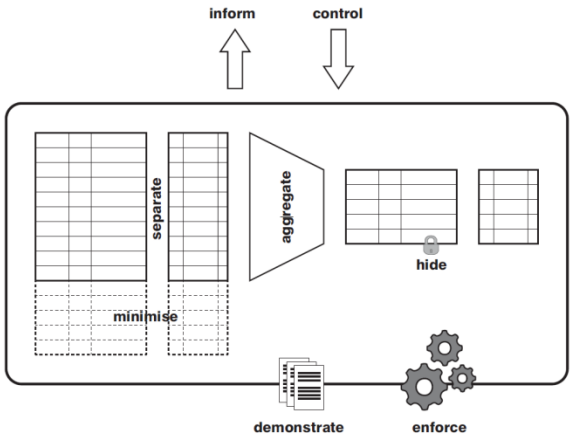
2.1.2 Privacy Design Strategies

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Privacy Design Strategies geven high-level richtlijnen voor het opstellen van een privacyvriendelijke systeemarchitectuur.	*Privacy Design Strategies zijn vooral toepasbaar in het ontwerpproces van een systeem of dienst waarin persoonsgegevens verwerkt worden.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Privacy Design Strategies hebben betrekking op het realiseren van privacy-vriendelijke oplossingen aan de hand van vastgestelde privacy-uitgangspunten	*De IT-afdeling en externe onderzoeks-/consultatiebureaus zijn verantwoordelijk voor de concrete ontwikkeling van Privacy Design Strategies. Afhankelijk van de reikwijdte van een te ontwikkelen systeem/dienst is commitment binnen de organisatie nodig.*

Bij het hanteren van een *Privacy by Design* ontwerpbenadering zijn verschillende oplossingen voor specifieke implementatieproblemen beschikbaar. Tussen de benadering van *Privacy by Design* en concrete oplossingen die bij de laatste fasen van ontwerp en implementatie bruikbaar zijn, zoals *Privacy Design Patterns*, zit echter een leemte. Om invulling te geven aan keuzes die gemaakt kunnen worden in eerdere fasen van een ontwerpproces, zoals conceptuele uitwerking en analyse,

werken onderzoeksinstellingen, waaronder het PI-lab, aan de uitwerking van *Privacy Design Strategies*..[22]

Op basis van de privacy-uitgangspunten die in wetgeving worden gehanteerd, is een initiële set van acht *Privacy Design Strategies* opgesteld: MINIMISE, SEPARATE, AGGREGATE, HIDE, INFORM, CONTROL, ENFORCE en DEMONSTRATE, die elk een basale strategie weergeven die bij het uitwerken van een ontwerp van een systeem wat persoonsgegevens verwerkt gehanteerd kan worden. In een artikel van Hoepman[23] zijn deze strategieën weergegeven op basis van een database-metafoor. Zo betekent de MINIMISE strategie dat er minder informatie over een persoon verzameld of verwerkt wordt, de AGGREGATE strategie dat persoonsgegevens zoveel als het doel toelaat in geaggregeerde vorm verwerkt moeten worden, en de INFORM strategie dat de persoon van wie persoonsgegevens verwerkt wordt hiervan adequaat op de hoogte gesteld moet worden.[24]



Figuur 1 – De acht strategieën weergegeven middels een database metafoor

Privacy Design Strategies zijn nog relatief nieuw en behoeven nog nadere uitwerking en beproeving. Niettemin bieden ze de mogelijkheid om de leemte die tussen de omvattende *Privacy by Design* benadering en concrete *Privacy Enhancing Technologies* in ligt nader in te vullen, wat vooral in de eerste stadia van een ontwerpproces van belang kan zijn.

[22] Daarmee wordt voortgebouwd op de 'privacy-by-policy' en 'privacy-by-architecture' aanpakken die Spiekermann en Cranor introduceerden. Zie Spiekermann, 2009, Engineering privacy http://www.informatik.uni-trier.de/~ley/db/journals/tse/tse35.html#SpiekermannC09

[23] Hoepman, J.-H. , 2012, Privacy Design Strategies, A preliminary version was presented at the Amsterdam Privacy Conference (APC 2012): http://www.cs.ru.nl/~jhh/publications/pdp.pdf

[24] Idem

Voorbeeld: Privacy Design Strategies

Voor ieder van de Privacy Design Strategieën zijn voorbeelden te geven. We geven er hier drie:

- Minimialiseren van gegevensverzameling heeft betrekking op het 'select before you collect' principe;
- Het scheiden van gegevens(-stromen) wijst in de richting van decentralisering van processen, zoals dit bij het Diaspora sociale netwerk wordt toegepast.
- Het aggregeren van data kan over tijd bij een individu of huishouden plaatsvinden (zoals bij de slimme ernergiemeters) of over locatie (zoals bij het verzamelen van verkeersgegevens).

Verder lezen:

- 'Select before you collect' Privacy Jacob Kohnstamm ebescherming van persoonsgegevens. De GRoene Amsterdammer,3 november 2010
- Diaspora: http://diasporaproject.org/

2.1.3 Privacy Design Patterns

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Faciliteren van privacyvriendelijke ontwerpkeuzes	*Bij ontwerp van een informatiesysteem wat persoonsgegevens verwerkt*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle verwerkingen van persoonsgegevens	*IT-verantwoordelijke, externe partij*

Een *Design Pattern* is een algemene herbruikbare oplossing voor een regelmatig voorkomend probleem bij het ontwerpen van software. Het is niet een concrete oplossing, maar een sjabloon wat aangeeft hoe een ontwerpprobleem aangepakt kan worden. Alhoewel het concept al langer bestaat, is het binnen de softwareontwikkeling pas echt populair geworden na de publicatie van het boek 'Design Patterns: Elements of Reusable Object-Oriented Software' van de zogenaamde Gang of Four.[25] *Privacy Design Patterns* lijken op de eerder omschreven *Privacy Design Strategies*, maar zijn concreter van aard en zullen meestal pas later in het ontwerpproces (bij de stap naar daadwerkelijke implementatie) van belang zijn.

Verschillende onderzoekers hebben dit idee toegepast op privacybescherming, door een aantal *Privacy Design Patterns* op te stellen: sjablonen voor het oplossen van veel voorkomende privacy problemen of -risico's in informatiesystemen. Zo worden *Privacy Preferences Helper Tool*, *Trust & Reputation Evaluation System*, en *Privacy Policy Negotiation* patterns geïntroduceerd door Dolinar[26], een *Privacy-Aware Network Client Pattern* door Pearson,[27] en o.a. *Informed Consent for Web-based*

[25] Gamma, 1995, Design Patterns: Elements of Reusable Object-Oriented Software

[26] Dolinar, 2009, Design Patterns for a Systemic Privacy Protection

[27] Pearson, 2010, Context-Aware Privacy Design Pattern Selection

Transactions door Romanosky.[28] Elk van deze *patterns* geeft een sjabloon voor een specifiek privacy gerelateerd probleem.

Op dit moment ontbreekt er echter één samenhangende, gezaghebbende collectie van *Privacy Design Patterns*. Door enkele partijen, voornamelijk onderzoekers, worden wel pogingen gedaan tot het verzamelen en standaardiseren van deze *patterns*, bijvoorbeeld door onderzoekers van de UC Berkeley School of Information op de website http://privacypatterns.org/, en door onderzoekers van het Retina project op de website http://www.privacydesignpatterns.org/. Het ontbreken van een gestructureerd standaardwerk of standaardverzameling op dit gebied maken *Privacy Design Patterns* nog lastig om toe te passen door ontwerpers. Over daadwerkelijke toepassing van *Privacy Design Patterns* is daarom nog weinig bekend.

2.1.4 Privacy Enhancing Technologies

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Technologische garanties voor het veilig verwerken van persoonsgegevens	*Bij ontwerp van informatiesysteem of als lapmiddel*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle geautomatiseerde verwerkingen van persoonsgegevens	*Management, IT-verantwoordelijke*

Privacy Enhancing Technologies (PET's), zijn technologische oplossingen en tools die geïntegreerd worden in informatiesystemen en daarbij helpen om de privacy en informatiebeveiliging te verbeteren, bijvoorbeeld door zwakke punten in een systeem te ondervangen. In veel gevallen is een PET een reactie op een bestaand technologisch gegeven dat een bedreiging voor de privacy vormt. Die bedreiging wordt door de PET weggenomen of verkleind. PET's zijn dus een algemeen concept dat in concrete technologieën wordt uitgewerkt. De exacte werking is afhankelijk van de specifieke technologie die een uitwerking vormt van het concept. Veel PET's worden ontwikkeld door universiteiten en bedrijven in onderzoeksprogramma's. Ook individuele programmeurs of privacy groepen ontwikkelen PETs.

Voorbeeld: Privacy Enhancing Technologies - Witboek voor beslissers

In 2004 schreef KPMG in opdracht van het ministerie van Binnenlandse Zaken een "witboek" over PET met als doel beslissers te stimuleren PET toe te passen om persoonsgegevens veilig te verwerken. Als voorbeelden van PET worden onder andere genoemd versleuteling, logische toegangsbeveiliging, het scheiden van identificerende gegevens van andere gegevens in gescheiden domeinen en anonimiseren van persoonsgegevens.

Het witboek beargumenteert dat de eenmalige en structurele kosten die aan de toepassing van PET zijn verbonden snel terugverdiend worden door kostenreductie en kwaliteitsverbetering.

Meer lezen over het witboek:
http://www.cbpweb.nl/downloads_technologie/witboek_pet.pdf

[28] Romanosky, 2006, Privacy Patterns for Online Interactions

2.1.5 Userinterface ontwerp voor privacy

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Transparantie en controle over de verwerking van persoonsgegevens bieden aan de gebruiker	*Bij het ontwerp van informatiesysteem*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Verzamelen, verantwoording	*IT-verantwoordelijke*

Oplossingen voor privacybescherming richten zich vaak op de technologie zoals bij het gebruik van encryptie of het anonimiseren van data. Een onderbelicht en op de gebruiker gericht aspect van privacybescherming in informatiesystemen is het ontwerp van de *userinterfaces*. Recentelijk heeft privacy onderzoeker Ira Rubinstein de aandacht gevestigd op deze kant van privacybescherming als een belangrijke voorwaarde voor het invullen van een principe als openheid over de wijze waarop met persoonsgegevens omgegaan wordt.[29]

Richtlijnen voor een privacy-vriendelijk userinterface ontwerp zijn nog niet breed toegepast, maar al wel enige tijd beschikbaar. Zo hebben onderzoekers al in 2004 een set valkuilen geformuleerd die een ontwerper dient te vermijden:

1. *Designs should not obscure potential information flow (because informed use of a system requires that user understand the scope of its privacy implications);*
2. *Designs should not conceal actual information flow (because users need to understand what information is being disclosed to whom);*
3. *Designs should not require excessive configuration to manage privacy but rather should enable users to practice privacy as a natural consequence of their normal engagement with the system;*
4. *Designs should not forgo an obvious, coarse-grain mechanism for halting and resuming disclosure; and*
5. *Designs should not inhibit users from transferring established social practice to emerging technologies.*[30]

De uitgangspunten die hier geformuleerd worden komen neer op transparantie, controle voor de gebruiker en rekening houden met de sociale normen rond privacy. Een andere set richtlijnen voor user-interface ontwerp met privacy in gedachten is meer in positieve zin geformuleerd door Lipford et al., toegespitst op sociale netwerksites:

1. *Make information flows more transparent, so that users know what information they are sharing and with whom;*
2. *Increase user awareness of information flows as they make decisions about sharing profile data, photos, and the like, both with other users and/or third parties;*

[29] Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. New York.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128146

[30] Lederer, et al., 2004, Personal Privacy through Understanding and Action: Five Pitfalls for Designers, in 8 PERSONAL & UBIQUITOUS COMPUTING 440
http://link.springer.com/article/10.1007%2Fs00779-004-0304-9

3. *Increase user awareness of how much information is archived and still available to others;*
4. *Make information and context concrete by providing specific examples of who will see what;*
5. *Provide more granular controls over information flows; and*
6. *Do not abruptly modify the flow of information.*[31]

Het toepassen van deze principes veronderstelt dat de ontwerper van het informatiesysteem begrip heeft van de betekenis van privacy voor de gebruikers van het informatiesysteem, de normen die zij daarbij hanteren en hoe het systeem daar op ingrijpt.

Voorbeeld: Google Circles

Een – vanuit privacy oogpunt gezien – succesvol user interface concept wat aan deze richtlijnen invulling geeft is Google Circles. Google biedt een sociale netwerk dienst aan genaamd Google+, waarbij gebruikers o.a. berichten met elkaar kunnen delen. Om gebruikers meer inzicht te geven in welk bericht met wie gedeeld wordt kunnen gebruikers hun contacten op intuïtieve wijze onderverdelen in "cirkels", zoals collega's, vrienden of familie. Bij het delen van een bericht kan de gebruiker dan eenvoudig zien en kiezen met wie het bericht gedeeld gaat worden. Andere sociale netwerksites hebben soortgelijke mechanismen geïmplementeerd.

Meer lezen over het Google Circles:
http://www.google.com/+/learnmore/circles/

2.1.6 Anonimisering en pseudonimisering

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Anonimisering en pseudonimisering zijn technische hulpmiddelen die het onmogelijk of moeilijker maken om gegevens terug te herleiden naar een persoon.	*Anonimisering/pseudonimisering wordt gebruikt in die gevallen waar de identiteit van een persoon niet strikt noodzakelijk is voor het leveren van een dienst.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Anonimisering/pseudonimisering heeft betrekking op het verwijderen van identificerende gegevens van een persoon. Bij pseudonimisering blijft een koppeling achteraf mogelijk.	*De IT-verantwoordelijke geeft aan waar anonimisering/pseudonimisering mogelijk is. De PO en FG kunnen dit proces ondersteunen en sturen.*

Volgens de Wet bescherming persoonsgegevens (Wbp) is een persoonsgegeven 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Hieruit volgt ook dat

[31] Heather Richter Lipford, et al., Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites, Proceedings of the 2009 International Conference on Computational Science and Engineering (2009)

gegevens die *niet* te herleiden zijn tot een persoon dan ook geen persoonsgegevens zijn en dus niet binnen de Wbp vallen. Anonimisering is het idee dat persoonsgegevens zodanig bewerkt of geaggregeerd kunnen worden dat ze op geen enkele manier te herleiden zijn tot de persoon waar ze betrekking op hebben, bijvoorbeeld door identificerende gegevens uit een dataset te verwijderen. Na anonimisering kunnen de gegevens dan zonder risico's voor de privacy van individuen verwerkt of gepubliceerd worden. Het CBP noemt anonimisering in de richtlijnen voor het beveiligen van persoonsgegevens 'de zwaarste vorm van Privacy Enhancing Technology'.[32]

In de praktijk is anonimisering van persoonsgegevens in veel gevallen mogelijk, al kan er ook een aantal kanttekeningen worden geplaatst. Zo kan na anonimisering de kwaliteit van de data onvoldoende zijn voor het doel waarvoor de data gebruikt moet worden. Daarnaast volstaat het eenvoudigweg verwijderen van de voor de hand liggende identificerende gegevens zoals naam, adres of BSN uit de data in veel gevallen niet. En in veel gevallen is het niet vanzelfsprekend wanneer gegevens te herleiden zijn naar een persoon. Is bijvoorbeeld identificatie mogelijk door de dataset te relateren aan andere al dan niet publieke datasets of gegevens? Het is niet altijd makkelijk om vast te stellen of gegevens geanonimiseerd zijn.[33] Bovendien wordt er tegenwoordig zelfs vaak gesteld dat anonimisering helemaal niet meer mogelijk is, aangezien gegevens vrijwel altijd tot een persoon herleid kunnen worden, gezien de veelheid aan gegevens en de technische mogelijkheden voor het linken van verschillende databronnen.[34] [35]

Bij pseudonimisering worden de velden in een dataset die een individu kunnen identificeren (bijvoorbeeld een naam, BSN, woonadres of IP-adres) vervangen door een 'pseudoniem': een kunstmatige identificatie die niet of moeilijk terug te leiden is op een individu. Dit pseudoniem kan ook gegenereerd worden door de oorspronkelijke identificerende gegevens te 'hashen' (waarmee ze omgezet worden in een zeer lastig terug te herleiden unieke code). Zoals het CBP constateert is deze vorm van pseudonimisering in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Daarmee is pseudonimisering niet hetzelfde als anonimisering, omdat niet volledig uit te sluiten valt dat de gegevens terug te leiden zijn op een persoon.

Ondanks de kanttekeningen die bij anonimisering en pseudonimisering zijn te plaatsen, zijn beide *best practices* die hun toepasbaarheid en toegevoegde waarde in de praktijk uitgebreid bewezen hebben. Ook als er geen volmaakte vorm van anonimisering mogelijk is kan het toepassen ervan de risico's nog steeds significant verkleinen.[36]

---

[32] CBP, 2013, Richtsnoer beveiliging van persoonsgevevens
http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[33] UK ICO, 2012, Anonymisation: managing data protection risk code of practice
http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx

[34] Article 29 working group, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, p. 19: "After that period this UDID should be further anonymised while taking into account that true anonymisation is increasingly hard to realize and that the combined location data might still lead to identification."

[35] Tucker, 2013, Has Big Data Made Anonymity Impossible? http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/

[36] Cavoukian, 2011, Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy: http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1084

We hebben anonimisering en pseudonimisering hier bekeken vanuit het perspectief van de data verwerker. Ze kunnen echter ook gezien worden als oplossingen die deel uit kunnen maken van de combinaties van oplossingen voor zelfredzaamheid, waarbij het subject beslist deze te gebruiken in bepaalde situaties of juist niet.

Voorbeeld: Google Analytics anonimisering

Google Analytics biedt sinds mei 2010 de mogelijkheid aan website eigenaren om de IP-adressen van de bezoekers van deze websites te anonimiseren. Google doet dit door in een zo vroeg mogelijk stadium bij de betreffende IP-adressen de laatste byte (bij IPv4 adressen) of de laatste 80 bits (bij IPv6 adressen) op nul te zetten. Daardoor zijn de achterliggende IP-adressen niet meer herleidbaar.

Dit is een beperkte vorm van anonimisering, aangezien de overgebleven gegevens van het IP-adres nog steeds informatie geven over de geografische plaats van de gebruikers. Desalniettemin biedt het eigenaren van websites de mogelijkheid om aan gebruikerseisen en eisen voortkomende uit bepaalde wettelijke regimes te voldoen.

Verder lezen:

https://support.google.com/analytics/answer/2763052

2.1.7 Anonymous credentials

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Anonymous credentials dienen om beweringen over een gebruiker aan te tonen(bijvoorbeeld een 18+ leeftijdscategorie) zonder de identiteit van de persoon vrij te geven.	*Voorbeelden van gebruik zijn leeftijdsverificatie (bij alcohol of sigaretten, het afnemen van bepaalde internetdiensten (gokken, adult content). In principe zijn anonymous credentials toepasbaar in iedere situatie waarin rechten moeten worden vastgesteld zonder dat de identiteit van de rechthebbende onthuld hoeft te worden.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Anonymous credentials hebben betrekking op het vermijden van het vrijgeven van identificerende gegevens, boven wat strikt noodzakelijk is voor een dienst.	*Anonymuos credentials zijn onderdeel van een systeemontwerp. Ze hebben impact op het business model omdat niet alle identificerende informatie verzameld zal worden, en daarmee niet alle business mogelijkheden benut kunnen worden. Dit valt onder de gezamenlijke verantwoordelijkheid van IT-ontwerpers/-beheerders, managers en directie.*

Anonymous credentials kunnen gebruikt worden om autorisaties te controleren zonder de identiteit van de individuele persoon vrij te geven. Daarmee is het een vorm van dataminimalisatie, waarmee tevens privacyrisico's geminimaliseerd worden. Het is in veel gevallen immers voldoende om te weten dat iemand toegang tot iets mag hebben, ongeacht wie dat dan precies is. Iemand die beschikt over een anonieme credential geeft aan gerechtigd te zijn voor benutting van een dienst, zonder zijn/haar identiteit te onthullen. De credential zelf hoeft geen persoonlijke informatie te bevatten, maar kan een random nummer of letter-cijfercombinatie zijn.

Bij Attribute-Based Credentials geven de credentials aan dat iemand over bepaalde eigenschappen beschikt. Een bekende voorbeeld is de leeftijdsverificatie die wordt gebruikt in sigarettenautomaten: de eigenschap dat iemand 16 jaar of ouder is, is voldoende om te weten of iemand sigaretten mag aanschaffen. De geboortedatum hoeft niet ontsloten te worden.

De mogelijke toepassingsvormen van Attribute-Based Credentials worden momenteel verder onderzocht in onderzoeksprogramma's waar bedrijven en onderzoeksinstellingen in samenwerken.[37] De technologieën zijn geschikt voor producenten en ontwerpers van IT-gebaseerde diensten waarin gebruik wordt gemaakt van – een beperkte set van – identificerende gegevens. Het concept is uitgewerkt binnen diverse projecten, maar de praktische toepassing is nog erg beperkt. Er is in Nederland een toepassing geweest bij sigarettenautomaten, waarbij alleen nog met een bankpas betaald kon worden. Op de pas kon de gebruiker bij het postkantoor een leeftijdsverificiatie laten zetten die aangaf dat hij of zij 16 jaar of ouder was, die daarmee toegang gaf tot de sigarettenautomaten.

Voorbeeld: IRMA - I Reveal My Attributes

Een concrete uitwerking van het attribute-based credentials concept is het IRMA project wat door het PI.Lab wordt uitgevoerd. In het IRMA project krijgt de gebruiker een persoonlijke kaart met een foto erop waarvoor bij gebruik een PIN code nodig is die alleen de gebruiker weet. Met de kaart en pincode kan de gebruiker ervan allerlei zaken aantonen zonder zijn of haar volledige identiteit prijs te geven, bijvoorbeeld: "ik ben een student", "ik ben ouder dan 18" of "ik woon in Den Haag". De IRMA technologie is geïmplementeerd in een aantal prototypes, maar nog niet breed in de praktijk toegepast.

Meer lezen over deze case:
https://www.irmacard.org/irma/

2.1.8 Standaarden voor informatiebeveiliging

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Beveiliging van persoonsgegevens	*Inrichting van organisatie, ontwerp van informatiesysteem, audits achteraf.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*Management, IT-verantwoordelijke*

Bedrijven en overheden moeten bij de verwerking van persoonsgegevens voldoen aan de wettelijke normen zodat iedereen erop kan vertrouwen dat zijn of haar persoonsgegevens worden beveiligd. Standaarden voor informatiebeveiliging is een van de onderdelen van het handhavingsbeleid van het CBP. De standaarden omvatten 'passende technische en organisatorische maatregelen' om persoonsgegevens te beveiligen. De standaarden zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk.

[37] Zie bijvoorbeeld het ABC4Trust project, een project uit het zog. zevende kaderprogramma van de EU; https://abc4trust.eu/

De CBP omschrijft het doel van deze standaarden als volgt: *"De standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken. Daarbij heeft een organisatie de ruimte om de beveiliging van persoonsgegevens in te richten op de wijze en met de middelen die in de specifieke situatie van deze organisatie het meest passend zijn. Een organisatie dient hierbij altijd de rechten van de betrokkenen te waarborgen en er moet sprake zijn van adequate, vakkundig toegepaste beveiliging waarbij de organisatie optimaal benut wat het vakgebied informatiebeveiliging te bieden heeft."* [38]

Het toepassen van standaarden voor informatiebeveiliging is gangbaar, voorbeelden zijn de Code voor informatiebeveiliging of de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum. De Code voor informatiebeveiliging is een technologieneutrale beveiligingsstandaard voor het initiëren, implementeren, handhaven en verbeteren van de informatiebeveiliging in een organisatie. Onder deze standaard vallen niet de maatregelen voor een specifiek type verwerken of het gebruik van een specifieke technologie. Beveiligingsstandaarden die hier juist wel op ingaan zijn de Data Security Standaard van de Payment Card Industry voor de beveiliging van creditcardbetalingen[39] en de beveiliging van 'cloud computing' van het Amerikaanse National Institute of Standards and Technology. [40]

Beveiligingsstandaarden gelden ook voor webapplicaties en mobiele apparaten (CPB, 2013). Het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie heeft ICT-beveiligingsrichtlijnen[41] en mobiele apparaten beveiligingsrichtlijnen.[42]

[38] CBP, Richtsnoeren Beveiliging van persoonsgegevens, 2013.
http://www.cbpweb.nl/Pages/rs_publicatie_persgeg_internet.aspx

[39] PCI Security Standards Council, Data security standards overview
https://www.pcisecuritystandards.org/security_standards/index.php

[40] NIST, Cloud computing program
http://www.nist.gov/itl/cloud/index.cfm

[41] NCSC, ICT-beveiligingsrichtlijnen voor webapplicaties
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[42] NCSC, Beveiligingsrichtlijnen voor mobiele apparaten
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html

2.2 Inrichten van processen en organisatie

Welke oplossingen helpen management om een organisatie en de processen in die organisatie zodanig in te richten dat privacybescherming versterkt wordt?

Zoals al eerder besproken is privacybescherming in een dienstverlenende organisatie niet alleen een zaak van het gebruik van de juiste technologie. Minstens net zo belangrijk zijn organisatorische maatregelen zoals het inrichten van processen, aanwijzen van verantwoordelijkheden en bewustzijnstraining. Voor het borgen van privacybescherming in een organisatie zijn er ook *best practices* bekend, zoals Privacy Impact Assessments, het hanteren van een organisatiebreed privacybeleid, het inrichten van procedures en toekennen van verantwoordelijkheden en privacybewustzijnstraining.

2.2.1 Privacy Impact Assessments

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Privacy risico's inventariseren en oplossingen aandragen	*Bij ontwerp nieuw informatiesysteem of significante wijziging bestaand systeem*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*Management, IT-verantwoordelijke*

Een Privacy Impact Assessment (PIA) is een methodologie voor het inschatten en beoordelen van het effect op privacy dat een project, dienst, product of ander initiatief heeft. Vervolgens worden in overleg met de betrokkenen noodzakelijke herstelmaatregelen getroffen om de mogelijk gevonden negatieve effecten te minimaliseren. Een PIA is niet alleen een hulpmiddel; het is een proces waarmee liefst zo vroeg mogelijk begonnen moet worden, wanneer er nog mogelijkheden zijn om de uitkomsten van een project te beïnvloeden.[43] Een PIA kan echter ook toegepast worden op bestaande systemen. Doel van een PIA is niet alleen te zorgen dat een initiatief voldoet aan de dataprotectiewetgeving maar dat, voor zover mogelijk, alle negatieve gevolgen voor de privacy van individuen als gevolg van een project in kaart gebracht worden en geminimaliseerd worden. Voor organisaties is het doel van een PIA het op orde krijgen van processen, verhogen van vertrouwen van klanten en betrokkenen, en het voorkomen van incidenten en negatieve publiciteit.

Er zijn verschillende omschrijvingen van de PIA methodologie gangbaar. De meeste omvatten een aantal activiteiten: het in kaart brengen van het project, identificeren van informatiestromen, informatie verzamelen van alle betrokkenen, privacyrisico's identificeren, maatregelen nemen om de risico's te minimaliseren, een conformiteitscheck, rapportage en periodieke controle achteraf.[44]

De PIA methodologie is al in gebruik sinds het midden van de jaren negentig, met name in Australië, Canada, Nieuw-Zeeland en de Verenigde Staten. In Europa is het echter nog relatief nieuw: de toezichthouder in het Verenigd Koninkrijk introduceerde een eerste methodologie in 2007 en verbeterde deze in 2009,[45] en Ierland volgde in 2010 met een PIA aanpak voor de gezondheidszorg.[46]

---

[43] Wright, 2012, The state of the art in privacy impact assessment
http://www.sciencedirect.com/science/journal/02673649/28/1

[44] PIAF project, 2012, Recommendations for a privacy impact assessment framework for the European Union
http://www.piafproject.eu/ref/PIAF_D3_final.pdf

[45] UK Information Commissioner's Office, 2009, PIA Handbook v2
http://www.ico.gov.uk/pia_handbook_html_v2/html/0-advice.html

In de voorgenomen Algemene Verordening Gegevensbescherming is een verplichting voor verwerkers van persoonsgegevens opgenomen om in sommige gevallen een PIA uit te voeren.[47] PIA methodes worden tot nu toe voornamelijk ontwikkeld door toezichthouders en overheden, al zijn er inmiddels ook verschillende commerciële partijen die een PIA in hun aanbod hebben of hier advies over geven. De rijksoverheid publiceerde in 2013 een toetsmodel voor het uitvoeren van PIAs bij de Rijksdienst.[48]

Voorbeeld: PIA van wetsvoorstel ANPR

Op 12 februari 2012 stuurde minister Opstelten een wetsvoorstel naar de Tweede Kamer dat regelt dat door het hele land camera's gebruikt mogen worden om kenteken van voertuigen te registreren en op te slaan middels ANPR-technologie (automatische nummerplaatherkenning). Omdat dit voorstel betrekking had op het verwerken van grote hoeveelheden persoonsgegevens is bij het opstellen van dit wetsvoorstel een Privacy Impact Assessment uitgevoerd. Bij deze PIA is het wetsvoorstel geanalyseerd en een risico-inschatting gemaakt. Daarbij is ook gekeken naar maatregelen om risico's te beheersen. In de conclusies van de PIA worden een aantal mogelijke risico's genoemd, waaronder: verplaatsingseffecten en diefstal van kentekens/voertuigen, beveiligingsproblemen, onvoldoende transparantie en interpretatiefouten.

Meer lezen over deze PIA:
https://zoek.officielebekendmakingen.nl/blg-207622.pdf

Veel voorbeelden van uitgevoerde Privacy Impact Assessments zijn te vinden op:
http://www.piawatch.eu/pia-report

2.2.2 Binding Corporate Rules

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
BCRs dienen om binnen een (internationaal) bedrijf bindende afspraken te maken over hoe het bedrijf met – in dit geval – persoonsgegevens om wil gaan.	*BCRs worden gebruikt om een bepaalde houding van het bedrijf uit te dragen, en in geval van grensoverschrijdend verkeer, om juridische onduidelijkheden (door verschillende wettelijke regimes) te ondervangen.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Binding Corporate Rules hebben in deze omstandigheid te maken met het gehele gegevensverwerkende proces. Ze kunnen worden toegespitst op die onderdelen die het bedrijf van belang acht.	*Het gaat hier om bedrijfspolicy. Dat behoort tot de competentie van de directie.*

[46] Health Information and Quality Authority, 2010, Guidance on Privacy Impact Assessment in Health and Social Care http://www.hiqa.ie/resource-centre/professionals

[47] Europese Commissie, 2012, Proposal to a General Data Protection Regulation http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[48] Rijksoverheid, 2013, Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html

Om tot privacybescherming in een organisatie te komen is het essentieel dat het topmanagement van de organisatie uitdraagt dat er belang wordt gehecht aan privacy, en daar in beslissingen ook invulling aan geeft. Een invulling van deze best practice is de praktijk van *binding corporate rules*. Binding corporate rules (BCR's) zijn een vorm van zelfregulering waarmee bedrijven een algemeen kader voor zichzelf scheppen over de manier waarop zij met gegevens omgaan. Dat geldt voor het gehele bedrijf, ongeacht de locatie. BCR's zijn dus met name interessant voor grote bedrijven, zoals multinationals met vestigingen over de hele wereld.

Het concept bestaat al langer en wordt veelvuldig gebruikt om regels binnen bedrijven vast te leggen. Dergelijke regels kunnen voor verschillende gebieden worden opgesteld, zoals faire behandeling van werknemers of het gebruik van eerlijke en duurzame producten. Met name de laatste jaren is de discussie toegenomen over BCR's en de rol die deze kunnen spelen met het oog op conformiteit met regelgeving op het gebied van dataprotectie. Er wordt aan BCR's gewerkt binnen diverse bedrijven, brancheverenigingen en belangenorganisaties. In academische kringen is nagedacht over de rol en functie, bijvoorbeeld in het proefschrift van Lokke Moerel uit 2011.[49]

Voorbeeld – Binding Corporate Rules

Het proefschrift van Lokke Moerel gaat in op de huidige praktijk van gegevensvergaring en –verspreiding waarbij steeds vaker sprake is van internationaal opererende bedrijven die persoonsgegevens van klanten uit verschillende landen verzamelen. Deze gegevens worden beheerd in centrale IT-systemen die niet noodzakelijk in het land van herkomst van de persoonsgegevens staan. De bewerking en verspreiding van de gegevens is vervolgens uitbesteed aan derde partijen die zich op weer een andere locatie bevinden. Daardoor hebben deze bedrijven te maken met een complex geheel aan wettelijke regelingen. Door het opstellen van Binding Corporate Rules pogen deze bedrijven aan de verschillende toezichthouders inzichtelijk te maken hoe met de persoonsgegevens wordt omgegaan en op deze wijze sanctionering van de praktijken te bewerkstelligen.

Meer lezen:

Lokke Moerel (2011). *Binding Corporate Rules. Corporate self-regulation of global data transfers.* Oxford University Press, Oxford.

2.2.3 Privacy Maturity Model

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Inrichten van processen en organisatie rond privacybescherming	*Bij het inrichten van een organisatie, in operationele fase, en bij audits achteraf.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*Directie, Management, IT-verantwoordelijke*

Het *Privacy Maturity Model*, opgesteld door de Amerikaanse en Canadese verenigingen van accountants AICPA en CICA, richt zich op het professionaliseren van de organisatorische kant van

[49] Lokke Moerel, 2012, Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers

privacybescherming. Dit *Maturity Model* is gebaseerd op het al langer bestaande *Capability Maturity Model*, wat onder andere in 1989 door de onderzoeker Watts Humphrey aan de Carnegie Mellon University in het boek *Managing the Software Process* is uitgewerkt.[50] Het *Capability Maturity Model* is een manier om de processen van een organisatie te ontwikkelen en verfijnen. Evenzo biedt het *Privacy Maturity Model* een manier om de processen rond privacybescherming in de organisatie te verbeteren. Het *Privacy Maturity Model* van AICPA en CICA is gebaseerd op 10 *Generally Accepted Privacy Principles (GAPP)* die deze organisaties hanteren als uitgangspunt, die uitgewerkt zijn tot 73 concrete, meetbare criteria.[51]

In dit model wordt onderscheid gemaakt tussen vijf niveaus van 'volwassenheid' die een organisatie kan hebben in de bedrijfsvoering, gemeten op een reeks criteria. Deze niveaus zijn (vertaald) ad-hoc, herhaalbaar, omschreven, beheerst, geoptimaliseerd. Op het laagste niveau, ad-hoc, zijn processen en procedures informeel, incompleet, en worden ze inconsistent toegepast. Op het hoogste niveau, geoptimaliseerd, zijn processen en procedures volledig en consistent gedocumenteerd en geïmplementeerd, en vindt dankzij regelmatige feedback en reviews voortdurend verbetering plaats. Een *maturity model* stelt geen norm of eis waaraan een organisatie moet voldoen; een organisatie maakt zelf een afweging tussen de noodzaak om op een vlak een bepaald maturiteitsniveau te bereiken en de investeringen die dit met zich mee brengt.

In onderstaande figuur is een uitwerking van één van de 73 GAPP criteria tot in het *Privacy Maturity Model* weergegeven. Op analoge wijze zijn de overige criteria in het model uitgewerkt.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.

Figuur 2 – voorbeeld uit het ACIPA-CICA Privacy Maturity Model

Het hier omschreven *Privacy Maturity Model* is in de Verenigde Staten en Canada opgesteld, en afgestemd op de daar geldende regelgeving. Voor Europa of Nederland is een dergelijk model op dit moment niet beschikbaar. Het is niet duidelijk in welke mate het model daadwerkelijk gebruikt wordt in de VS en Canada.

2.2.4 Functionaris gegevensbescherming

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Aanspreekpunt en handhaving rond privacy beleid van organisatie	*Voortdurend*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*Directie, Management*

Het privacy maturity model heeft als één van de criteria waarop volwassenheid gemeten wordt de mate waarin verantwoordelijkheden voor het organiseren en controleren van maatregelen ter

[50] Humphrey, 1989, Managing the Software Process

[51] ACIPA-CICA, 2011, Privacy Maturity Model
http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/pages/aicpacicaprivacymaturitymodel.aspx

bescherming van privacy toegekend zijn. Een functionaris gegevensbescherming (FG) is een voorbeeld hiervan; de persoon met deze functie binnen een bedrijf of organisatie is verantwoordelijk voor het correct implementeren van het beleid en de wettelijke privacy regels.[52] De FG ontwerpt het privacybeleid.[53]

Een FG in Nederland heeft de verantwoordelijkheid om binnen de organisatie toezicht te houden op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De organisatie, overheid of instelling stellen zelf een FG aan, een "interne toezichthouder op de verwerking van persoonsgegevens". "Alle betrokkenen van wie persoonsgegevens verwerkt worden, zoals klanten, patiënten en personeelsleden, kunnen bij een FG terecht voor informatie over en inzage in de eigen verwerkte persoonsgegevens of voor klachten."[54] Een eis van de Wbp is dat deze functionaris beschikt over "toereikende kennis van de privacyregelgeving en betrouwbaar is. "Een functionaris voor de gegevensbescherming vergroot het privacybewustzijn binnen een organisatie en levert een bijdrage aan het realiseren van een betere bescherming van de persoonlijke levenssfeer".[55]

Voorbeeld: Functionaris gegevensbescherming in de zorg

Zorginstellingen zijn bij uitstek organisaties waarin gevoelige persoonsgegevens verzameld, bewaard en verwerkt worden. Een functionaris gegevensbescherming is dan ook een zeer relevante rol binnen zorginstellingen. In een artikel uit 2011 in het Zorgvisie magazine wordt deze rol in de context van zorginstellingen nader uitgewerkt. Zo wordt besproken hoe specifieke zorginstellingen vrijgesteld zijn van de meldingsplicht voor het verwerken van persoonsgegevens: beoefenaren van individuele beroepen in de gezondheidszorg, verzorgingshuizen en verpleeghuizen. Ook wordt benadrukt dat een functionaris gegevensbescherming duidelijk onderscheiden moet zijn van een *security officer*.

Lees het artikel online:
http://www.zorgvisie.nl/Kwaliteit/Verdieping/2011/4/Persoonsgegevens-in-goede-handen-bij-FG-ZVS011188W/

[52] Karjoth G. and Schunter M., 2002. A privacy policy model for enterprises, IBM Research, Zurich Research Laboratory, Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE, pp 271 - 281

[53] Günter Karjoth, Matthias Schunter, Michael Waidner, 2003. Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data, Springer Berlin Heidelberg, pp 69-84

[54] CPB, 2012. Functionaris voor de Gegevensbescherming (FG)
http://www.cbpweb.nl/Pages/ind_wetten_zelfr_fg.aspx

[55] CPB, 2012. De functionaris voor de gegevensbescherming Informatieblad nummer 16,
http://www.cbpweb.nl/Pages/inf_va_fg.aspx#1

2.2.5 Training en bewustzijn

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Training en bewustzijn dient om de gevoeligheid binnen de organisatie voor het omgaan met persoonsgegevens te vergroten en up to date te houden.	*Het trainen van medewerkers en activiteiten voor het vergroten van het bewustzijn van medewerkers kan in iedere fase van systeem-/ dienstontwikkeling en –gebruik worden toegepast.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Training en bewustzijn hebben betrekking op het vergroten van kennis en inzicht in functies, rollen en verantwoordelijkheden rond de verwerking van persoonsgegevens binnen een organisatie.	*Management en directie zijn initieel verantwoordelijk.*

Trainingen voor privacybewustzijn zijn een middel om medewerkers bewust(er) te maken van de risico's die verbonden zijn aan schendingen van de privacy en om de bescherming van persoonsgegevens te verbeteren.[56] Het is nuttig om onderscheid te maken tussen BCR's, die bindende afspraken omvatten waaraan medewerkers zich moeten houden, en trainingen die het bewustzijn van medewerkers verhogen zonder dat dit noodzakelijk resulteert in concreet na te leven regels en richtlijnen.

Trainingen voor privacybewustzijn worden door meerdere instanties gegeven. Voorbeelden zijn de afdeling gezondheid en menselijke diensten in het DHS Cybersecurity programma in de Verenigde Staten. Doel van de training is het bewustzijn te vergroten voor een goede omgang met persoonsgegevens en een geode afscherming van de privacy van betrokkenen: belang, wetten, beleid, principes, de rol van een organisatie/burger in de bescherming van privacy, consequenties voor overtredingen, bescherming en het herkennen van potentiele bedreigingen.[57] In de Verenigde Staten komen in toenemende mate wetten en regelingen beschikbaar die activiteiten voor de vergroting van privacybewustzijnvereisen.[58]

[56] Herold, R. 2011. Managing an information security and privacy awareness and training program. Second edition. CRC Press Taylor & Francis Group, LLC

[57] HHS Cybersecurity Program, 2013. The Department of Health and Human Services (HHS) Privacy Awareness Training http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/privacyawarenesstraining.pdf.

[58] Herold, R. 2011. Managing an information security and privacy awareness and training program. Second edition. CRC Press Taylor & Francis Group, LLC

Voorbeeld: Trainingen voor een bewustere omgang met persoonsgegevens en privacy

Verschillende organisaties bieden cursussen aan die gericht zijn op het bevorderen van het privacybewustzijn binnen bedrijven. In de regel betreft het cursussen en instrumenten die bedrijven helpen bij het vaststellen of men conform de wettelijke richtlijnen opereert. Maar in toenemende mate komen er ook cursussen die gericht zijn op het bevorderen van privacybewustzijn op de werkvloer. Soms betreft het eenpitters met een adviesbedrijf, in andere gevallen betreft het branchegerichte kenniscentra.

Zie ook:

- NIBE-SVV Kenniscentrum voor de financiële wereld: http://www.nibesvv.nl/Opleidingen
- De Privacypraktijk, advisering over privacy: http://www.deprivacypraktijk.nl/
- Het NederlandsPrivacy Instituut: http://www.n-pi.org/tag/in-company-privacy-trainingen/

2.3 Vertrouwensnetwerken

Welke oplossingen stellen groepen van stakeholders in staat om gezamenlijk tot een vertrouwenwekkende bescherming van persoonsgegevens te komen?

Vertrouwensnetwerken zijn systemen die in een bepaalde omgeving (context zoals medische verzorging, ouderenzorg, banken, vereniging of club, een bepaald bedrijf) vertrouwen opbouwen en beheren zodat de gebruikers, leveranciers en anderen op een betrouwbare manier transacties met elkaar kunnen uitvoeren.

In het kader van dit Actieplan gaat het om vertrouwensnetwerken die digitale transacties regelen. Uitgangspunt is dat de eindgebruiker (consument, patiënt, maar ook bedrijven of organisaties als eindgebruikers) betrokken is bij het beheer over zijn persoonlijke data. Dat wil zeggen dat de data van de eindgebruiker veilig is opgeslagen en niet gebruikt of opgeslagen kan worden door een andere partij zonder de expliciete toestemming (sleutel) van de eindgebruiker. De eindgebruiker kan algemene toestemming geven of elk geval apart bekijken. Een vertrouwensnetwerk wordt zo georganiseerd dat de gebruiker zo min mogelijk met elk specifiek geval van persoonlijk datagebruik wordt geconfronteerd.

Voorbeelden van dergelijke vertrouwensnetwerken zijn:

- Een platform voor gezondheidszorg, waarin ziekenhuizen, verzekeraars, overheid, patiënten, verplegers, artsen, leveranciers zijn samengebracht.
- Een platform voor Human Capital management binnen een regio waarin bedrijven (werkgevers), arbeidsbemiddeling, onderwijsinstellingen en studenten en werknemers samen werken aan een zo goed mogelijk match van beschikbare arbeid en arbeidskrachten.

We onderscheiden twee typen vertrouwensnetwerken waarbij in beide gevallen wordt aangenomen dat de eindgebruiker een eigen gegevenskluis heeft (centraal of in de cloud maar alleen toegankelijk met toestemming (sleutel) van de eindgebruiker):

One2many

De transacties vinden typisch plaats tussen één grote organisatie en vele eindgebruikers. De grote organisatie kan op zijn beurt bestaan uit een vereniging van organisaties. De organisatie legt contractueel vast hoe gebruik kan worden gemaakt van de persoonlijke data van de eindgebruiker. Op basis hiervan wordt een interface geïmplementeerd en beheerd (door derden) die de contractuele keuzes respecteert en garandeert. Dit gebeurt door een combinatie van technische en beheersmatige (governance) middelen. Voorbeelden van zulke vertrouwensnetwerken zijn een grote retailer met zijn loyalty klanten, een groot bedrijf met werknemers, of een groep banken met hun klanten. Door middel van standaardisatie van regels en procedures is het mogelijk om tot reproduceerbare implementatiestrategieën te komen.

Voorbeeld: Qiy

De Nederlandse stichting Qiy presenteert zichzelf als "tegenbeweging op de wildgroei aan digitale data". De gedachte achter Qiy is het teruggeven van de controle over persoonsgegevens aan de betrokkenen. Qiy doet dit niet door het creëren van een centrale database (een zogenaamd persoonlijke gegevenskluis, zie verderop) maar door het leggen van verbanden tussen de verschillende databases waarin persoonsgegevens van een betrokkene worden opgeslagen en gebruikt. Zo bepaalt de betrokkene zelf welke data in welke omgeving voor welk doel kan worden gebruikt.

Verder lezen over deze case:

- https://www.qiyfoundation.org/nl/

Many2many

De transacties vinden plaats binnen een vertrouwensnetwerk bestaande uit diverse stakeholders, zoals grotere organisaties of overheidsinstellingen, leveranciers, eindgebruikers en de belangengroepen van deze stakeholders, etc. Een *voorwaardenscheppende ecosysteeminfrastructuur* (platform) is beschikbaar voor de uitvoering van de diverse transacties tussen de verschillende leden conform vooraf vastgelegde principes en contractueel onderbouwde transacties. De technische en beheersmatige implementatie is gericht op het scheiden van authenticatie en autorisatie, en het gebruiken van pseudoniemen in plaats van reële identiteiten.. Typische voorbeelden van afspraken op zo'n platform zijn:

(1) toepassing van standaardprocessen die minimaal datagebruik garanderen en

(2) kopiëren van data onmogelijk maken,

(3) transactie logging, auditing en controle op correctheid (bijvoorbeeld door random tests uit te voeren op conformiteit van processen).

Bovendien wordt een beheerstructuur gebruikt waarin via 'separation of concern' een onafhankelijke groep van experts wordt aangesteld (door de stakeholders) die toeziet op de activiteiten en structureel audits verzorgt.

In deze structuur zijn het stakeholders die services inbrengen waarbij ze zich verplichten tot de regels van het platform. Hierbij is het essentieel dat data en datagebruik veilig is binnen het platform. In een gebruikersnetwerk

2.3.1 Digitale persoonsgegevenskluis

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Controle over persoonsgegevens bij gebruiker	*Delen en verwerken van persoonsgegevens*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*Gebruiker*

Een digitale kluis voor persoonsgegevens biedt de mogelijkheid om persoonsgegevens digitaal op te slaan en deze middels een beveiligingsmechanisme gecontroleerd ter beschikking te stellen aan

derden. De digitale kluis is de Nederlandse benaming van de meer generieke term user-controlled personal data management. Bij user-controlled personal data management services bepaalt de gebruiker met wie persoonlijke gegevens of persoonsgegevens gedeeld worden. Hij of zij heeft dus zelf de verantwoordelijkheid voor persoonsgegevens.

Recent is de toevoeging aan dergelijke diensten dat ze gebruikt kunnen worden om geld te verdienen met persoonsgegevens. Het idee is dat steeds meer bedrijven bereid zijn om te betalen voor persoonsgegevens en dat de personen aan wie de gegevens toebehoren deze gegevens dus naar eigen wens kunnen delen of juist verbergen om meer of minder geld te verdienen.

Het "selling point" van user-controlled personal data management services is dat gebruikers zelf controle hebben over hun persoonsgegevens en daarmee over hun privacy. Het concept is al langer in ontwikkeling en ligt in de lijn van gegevensmanagementprincipes als 'gegevens eenmalig opslaan bij de bron'.[59] Behalve dat het bestaat als privacy principe, zijn er inmiddels ook een aantal (commerciële) voorbeelden. Zowel universiteiten (Prometheus, ontwikkeld door de University of South Florida[60]), als toezichthouders (DPA Sleswig-Holstein[61]), als commerciële partijen (QIY, Synergetics, iCentered[62] [63]) hebben voorbeelden hiervan ontwikkeld (of eraan meegewerkt) voor consumenten of gebruikers van online diensten. Deze partijen bieden niet alleen een kluis voor persoonsgegevens, maar vaak ook ondersteuning voor de processen die de data uit de kluis kunnen gebruiken, waarmee ze het veilig en gecontroleerd ontsluiten van persoonsgegevens uit de kluis mogelijk maken.

Ook de Nederlandse overheid heeft al in 2001 nagedacht over het concept van een digitale kluis als onderdeel van de relatie burger-overheid.[64] De gedachte achter de digitale kluis was dat deze kan worden gebruikt door burgers om informatie te delen met verschillende overheden. Inmiddels is deze gedachte deels vormgegeven in MijnOverheid.nl. Hier kan de burger inzicht krijgen in welke gegevens de overheid over hem of haar bewaart, al zijn de controle mogelijkheden (vooralsnog) beperkt.

---

[59] Zoals besproken in Hansen, M. (2008) 'Marrying Transparency Tools with User-Controlled Identity Management', in: Fischer-Hibner, S., Duquenoy, P., Zuccato, A. & Martucci, L., IFIP Volume 262 'The Future of Identity in the Information Society' (Boston: Springer), pp. 199-220.

[60] Kourtellis, N., Finnis, J., Anderson, P., Blackburn, J., Borcea, C. & Iamnitchi, A. (2010) 'Prometheus: User-Controlled P2P Social Data Management for Socially-Aware Applications'.

[61] Hansen, M. (2008) 'Marrying Transparency Tools with User-Controlled Identity Management', in: Fischer-Hibner, S., Duquenoy, P., Zuccato, A. & Martucci, L., IFIP Volume 262 'The Future of Identity in the Information Society' (Boston: Springer), pp. 199-220.

[62] Icentered: http://www.icentered.com/

[63] Qiy: https://www.qiy.nl/

[64] Eindrapport "GBA in de toekomst". Commissie-Snellen, maart 2001

2.3.2 Sticky policies

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Sticky policies worden gebruikt afspraken over wat wel of niet met persoonsgegevens mag gebeuren vast te koppelen aan de gegevens zelf	*Tijdens de ontwerpfase.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle verwerkingen van persoonsgegevens	*De IT-verantwoordelijke, al dan niet in samenwerking met externe partijen verantwoordelijk.*

Sticky policies staat voor een ontwerpbenadering waarbij softwarematig regels worden gekoppeld aan (persoons-)gegevens. De regels bevatten de privacy policy; ze geven aan wat er met de gegevens gedaan mag worden en door wie. De gegevens zijn versleuteld. De policy heeft een machine-readable format, waardoor de policy als het ware automatisch gehandhaafd wordt. Bijvoorbeeld, bij het raadplegen van de gegevens wordt een verzoek voor de sleutel om de gegevens te ontsleutelen verstuurd naar een Trust Authority (TA). Die controleert of de verwerking is toegestaan en geeft of weigert de sleutel. Een verwerking die niet toegestaan is wordt geblokkeerd. Zo kan voorkomen worden dat de gegevens gekopieerd worden of dat er ongeautoriseerde toegang tot de gegevens plaatsvindt.

Voor de policies wordt aansluiting gezocht bij bestaande systemen, zoals het Platform for Privacy Preferences (P3P) van het World Wide Web Consortium (W3C). De gedachte achter Sticky policies (in 2003 gepresenteerd door ontwikkelaars van HP) is niet specifiek gericht op het bevorderen van privacyvriendelijke systemen. Verdere ontwikkeling van Sticky policies vindt plaats binnen onderzoeksinstellingen en het bedrijfsleven .

De toepassing is in potentie breed, omdat Sticky policies bruikbaar zijn voor alle elektronische gegevensverwerkingen. Het concept is vrij ver ontwikkeld en is wereldwijd bekend. Toepassing in concrete systemen blijft nog achter.

2.3.3 Context-aware privacy policies

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Verfijnde controle over delen en gebruik van persoonsgegevens	*Delen en verwerken van persoonsgegevens*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Alle aspecten van verwerking van persoonsgegevens	*IT-verantwoordelijke, gebruiker*

Bij het omgaan met persoonsgegevens wordt vaak een binair model gehanteerd dat onderscheid maakt tussen “publieke” en “private” (persoons)gegevens. De praktijk is echter minder eenvoudig: de normen die personen hanteren rond het delen van persoonsgegevens zijn afhankelijk van de context waarin informatie gedeeld wordt. Bijvoorbeeld, een persoon zal bij een bezoek aan de dokter vaak geen bezwaar hebben tegen het delen van gevoelige medische informatie, maar in een andere context zoals een sollicitatiegesprek juist wel. Zoals Helen Nissenbaum het omschrijft: *“For the myriad transactions, situations and relationships in which people engage, there are norms—*

explicit and implicit—governing how much information and what type of information is fitting for them."[65]

Het vertalen van dit idee van contextafhankelijke normen rond het delen van persoonsgegevens naar technologische implementatie is nog steeds een uitdaging. Een vertrouwensnetwerk waarin persoonsgegevens uitgewisseld wordt moet met deze context-afhankelijkheid om kunnen gaan. Anders gesteld: de *privacy policies* die bepalen welke partij onder welke voorwaarden of in welke context bij persoonsgegevens mag moeten context gevoelig zijn. Bijvoorbeeld: een *privacy* policy kan stellen dat alleen een arts en alleen voor urgente medische doeleinden bepaalde persoonsgegevens vrijgegeven mogen worden.

Context-gegevens die hierbij gehanteerd kunnen worden zijn bijvoorbeeld: activiteit, sociale context, locatie, tijd, fysieke toestand, omgevingsfactoren, mentale toestand of de toestand van een applicatie of apparaat wat de persoon gebruikt.[66]

De meeste systemen die persoonsgegevens verwerken bezitten een zekere (minimale) mate van context-bewustzijn, bijvoorbeeld door het hanteren van regels die alleen personen in bepaalde rollen toegang geven tot bepaalde gegevens. Meer uitgebreide context-aware privacy policies zijn sterk in ontwikkeling.

[65] Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy, 17(5/6), 559. doi:10.2307/3505189

[66] A. K. Dey, and G. D. Abowd, "Towards a better understanding of context and context-awareness," GVU technical report GIT-GVU-99-22, College Computing, GA Institute of Technology (1999).

2.4 Geïnformeerde instemming

Welke oplossingen kan een dienstverlener gebruiken om afnemers van een dienst goed te informeren over de wijze waarop met persoonsgegevens omgegaan wordt en ze daarin een betekenisvolle keuze te bieden?

Het wettelijk kader betreffende gegevensverwerking vereist een legitieme verwerkingsgrond. Voor de verwerking van persoonsgegevens geldt toestemming als één van de mogelijke verwerkingsgronden, bij gevoelige gegevens is het veelal de enige geoorloofde verwerkingsgrond. Toestemming is gedefinieerd als: "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt". Het op de juiste wijze verkrijgen van toestemming van het subject voor verwerking van zijn of haar persoonsgegevens in een bepaalde context is een wettelijk vereiste voor de verwerking.

In relatie tot toestemming kan gewezen worden op het gebruik van privacyverklaringen, als instrument ter verhoging van transparantie rondom de verwerking van persoonsgegevens, maar ook als instrument op basis waarvan een betrokkene de keuze kan maken al dan niet toestemming te verlenen voor de verwerking van persoonsgegevens. In zijn proefschrift verwijst Verhelst naar de Verenigde Staten als voorbeeld van een *best practice* in die zin dat daar gebruik wordt gemaakt van gestandaardiseerde privacyverklaringen. De Europese Commissie overweegt momenteel om ook binnen Europa te gaan sturen op gestandaardiseerde privacyverklaringen, toegespitst op het Europese juridische raamwerk.[67]

Voor het ondersteunen van *informed consent*, oftewel geïnformeerde instemming, zijn een aantal *best technologies* en *best practices* bekend. Allereerst zijn er de *best practices* van het ondersteunen van het recht om vergeten te worden, (of het recht om persoonsgegevens te laten wissen) en het bieden van begrijpelijke en stapsgewijze keuzemogelijkheden met behulp van *layered consent*. Daarnaast zijn er *best technologies* in ontwikkeling en gebruik zoals persoonsgegevensdashboards, manieren om de toegankelijkheid van privacy statements te verbeteren en access logs voor een betere verantwoording van de wijze waarop met persoonsgegevens is omgegaan.

2.4.1 Toegankelijke privacy statements

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Privacyverklaringen dienen transparantie over gegevensgebruik te bevorderen.	*Privacyverklaringen worden toegevoegd aan gegevensverwerkingsprocessen, op basis van een ontwikkeld systeem of dienst.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Privacyverklaringen geven aan op welke wijze de organisatie het verzamelen, beheer, de verwerking en verspreiding van persoonsgegevens geregeld heeft en welke rechten en plichten gelden.	*De privacy officer/functionaris van de gegevensverwerking dan wel andere daartoe bevoegde personen in samenspraak met de afdeling IT zijn verantwoordelijk voor de privacyverklaring.*

Een van de uitgangspunten van een verantwoordelijke omgang met persoonsgegevens is de mogelijkheden die de persoon waarover gegevens verwerkt worden heeft om voor deze verwerking al dan niet toestemming te geven. Toestemming geven is echter betekenisloos als de persoon in kwestie niet weet waarvoor hij of zij toestemming geeft: het uitgangspunt is dan ook geïnformeerde

[67] Op dit terrein zie je ook online diensten ontstaan, zoals bijvoorbeeld: http://www.generateprivacypolicy.com/

toestemming (*informed consent*). Van de persoon die van een dienst gebruik maakt, mag verwacht worden dat deze zich informeert, maar de verantwoordelijke voor het verwerken van persoonsgegevens moet de persoon over wie persoonsgegevens verzameld en verwerkt worden hierover goed en duidelijk informeren.

Het CBP noemt een aantal uitgangspunten voor deze informatieplicht voor verantwoordelijken voor de verwerking van persoonsgegevens: deze dient rekening te houden met de verwachtingen die de betrokkene redelijkerwijs kan hebben, de omstandigheden waaronder de gegevens verkregen worden (bijv. inkoop van een gegevenshandelsbureau), het beoogde gebruik van de gegevens en de gevoeligheid van de gegevens.[68] In de praktijk wordt aan deze informatieplicht vaak invulling gegeven door middel van een lange en ontoegankelijk geformuleerde *privacy statement* (privacyverklaring) bij websites of andere plaatsen waar persoonsgegevens verzameld worden. Een *best practice* rond privacyverklaringen is het streven naar toegankelijkheid van deze verklaringen. De uitdaging hierbij is het zowel volledig als toegankelijk formuleren van tekst, en het gebruik maken van hulpmiddelen zoals visualisatie en iconen om aan gebruikers duidelijk te maken wat er met persoonsgegevens gebeurt. Daarnaast kan er gebruik gemaakt worden van de, eerder genoemde, standaard privacyverklaringen.

Toegankelijke privacyverklaringen zijn nog geen gemeengoed, maar er zijn wel verschillende initiatieven die als doel hebben de toegankelijkheid ervan te vergroten. Een voorbeeld is het 'Terms of Service; Didn't Read' project, wat de algemene voorwaarden (waaronder ook privacyverklaringen) van verschillende diensten doorneemt en samenvat middels een aantal toegankelijke en vergelijkbare beoordelingen op een aantal sleutelpunten, zoals de vraag of een dienst wel of niet persoonsgegevens doorverkoopt aan derden.[69]

2.4.2 Ondersteunen van het 'recht om vergeten te worden'

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Vernietigen persoonsgegevens na wegvallen noodzaak tot bewaren	*(Langdurige) opslag van persoonsgegevens*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Archivering, opslag van persoonsgegevens	*IT-verantwoordelijke*

Eén van de uitdagingen rond privacy die digitalisering met zich mee brengt is dat het door o.a. de toenemende opslacapaciteit van digitale media steeds eenvoudiger wordt om persoonsgegevens langdurig te bewaren en veelvuldig te kopiëren. Voor personen over wie gegevens bewaard worden brengt dit risico's met zich mee omdat de kans op een lek of ongeoorloofd hergebruik van gegevens toeneemt. Een antwoord op deze uitdaging is geformuleerd als het 'recht om vergeten te worden': personen hebben het recht om op verzoek hun persoonsgegevens te laten wissen. Dit recht is ook in de voorgestelde Algemene Verordening Gegevensbescherming opgenomen.[70]

[68] CBP, 2012, Informatieblad Informatieplicht
http://www.cbpweb.nl/downloads_inf/inf_va_informatieplicht.pdf

[69] ToS;DR project, 2013, Terms of Service; Didn't Read Ratings
http://tosdr.org/

[70] EC, 2012, Proposed General Data Protection Regulation
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Een strikte interpretatie van het recht om vergeten te worden betekent dat alle kopieën van de data worden gewist, inclusief alle afgeleide data, en wel zodanig dat het herstellen ervan onmogelijk is met alle bekende technische middelen. Een minder strikte interpretatie laat het bewaren van versleutelde data toe als ongeautoriseerde partijen deze niet kunnen ontcijferen, en de meest losse interpretatie staat bewaren van data toe zo lang de data maar niet meer in publieke indexen of zoekmachines te vinden is.[71]

In de praktijk is het effectief realiseren van dit voorgestelde recht echter niet eenvoudig. Uitdagingen liggen in de (on)mogelijkheid voor individuen om vast te stellen waar hun data opgeslagen is, om alle kopieën en afgeleiden van data te traceren en om te bepalen of een persoon het recht heeft om een verzoek in te dienen om data te wissen.[72] Niettemin is het mogelijk om een 'recht om vergeten te worden' te ondersteunen in informatiesystemen waarin persoonsgegevens verwerkt worden.

Op dit moment zijn er verschillende oplossingen in ontwikkeling of beschikbaar rond het ondersteunen of automatiseren van het 'recht om vergeten te worden'. Deze worden echter nog niet breed toegepast, en hebben hun effectiviteit in de praktijk nog niet bewezen. Een idee wordt aangedragen door Mayer-Schoenberger, die voorstelt om gevoelige persoonsgegevens van een 'label' met een houdbaarheidsdatum te voorzien, waarbij alle computers die deze persoonsgegevens verwerken gebonden zijn om zich aan deze houdbaarheidsdatum te houden en de data na de datum te wissen.[73]

Voorbeeld: wissen persoonsgegevens in browsers

Bij het gebruik van een internet browser applicatie laat een gebruikers sporen na. Zo wordt een geschiedenis bijgehouden van de pagina's die een gebruiker bezoekt, wordt om het laden van pagina's te versnellen data opgeslagen in een cache, en worden o.a. zaken die in formulieren worden ingevuld zoals login namen en wachtwoorden opgeslagen. De meeste browsers bieden de mogelijkheid om het wissen van deze gegevens in meer of mindere mate geautomatiseerd te wissen. Alle browsers bieden de mogelijkheid om deze gegevens met de druk op één knop te wissen. Enkele browsers, zoals Firefox, staan het toe om deze gegevens na elk gebruik automatisch te laten wissen. Deze functionaliteit is een voorbeeld van het automatiseren van het recht om vergeten te worden.

[71] ENISA, 2011, The right to be forgotten – between expectations and practice https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport

[72] Idem

[73] Mayer-Schoenberger, 2007, Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976541

2.4.3 Gelaagde instemming

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Begrijpelijke en granulaire controle voor gebruiker over persoonsgegevens	*Voorafgaand aan verzamelen van persoonsgegevens*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Verzamelen, gebruik van persoonsgegevens	*IT-verantwoordelijke, Gebruiker*

Een probleem met het vragen van instemming aan de gebruiker is dat het in de praktijk vaak niet correct wordt ingezet. De onderzoeker Kosta concludeert in haar proefschrift dan ook dat er vele "worst practices" zijn in relatie tot het geven van instemming, en dat *best practices* nog nauwelijks waarneembaar zijn.[74] Kosta stelt dat de getrapte variant van informatievoorziening zoals beschreven door de artikel 29 werkgroep (WP100) een goed voorbeeld is. In deze variant zijn 3 trappen aanwezig: trap 1 betreft een korte kennisgeving, trap 2 een beknopte kennisgeving, en trap 3 volledige kennisgeving. Meer specifiek beschrijven Bunnik et al. het getrapte (layered) systeem in relatie tot 'informed consent in personal genome testing'.[75] In relatie tot onderzoek naar menselijk weefsel wordt een *tiered consent* variant gebruikt, waarbij het met name om het bieden van gelaagde keuzemogelijkheden lijkt te gaan.

Het doel van layered and tiered consent is om de burger een daadwerkelijk geïnformeerde keuze te laten maken met betrekking tot wat zij wel en niet willen in relatie tot de verwerking van persoonsgegevens. Waarden als transparantie en (geïnformeerde) keuzevrijheid staan hierbij centraal.

[74] Eleni Kosta, Unravelling consent in European data protection legislation - a prospective study on consent in electronic communications, dissertatie Leuven 2011.

[75] Bunnik EM, Janssens AC, Schermer MH., A tiered-layered-staged model for informed consent in personal genome testing, http://www.ncbi.nlm.nih.gov/pubmed/23169494

Voorbeeld: British Telecom website cookie controls

Een voorbeeld van een implementatie van gelaagde instemming, oftewel layered en tiered consent, is te vinden in het mechanisme wat British Telecom op haar website gebruikt om gebruikers controle te geven over de wijze waarop met cookies omgegaan wordt. De website biedt een mechanisme waarmee de gebruiker die “lagen” van instemming kan geven: elke laag omvat zowel instemming met de zaken die in de lagen eronder genoemd worden, als de zaken die in die laag zelf genoemd worden. De drie lagen zijn: strikt noodzakelijk, extra functionaliteit en personalisatie van advertenties. Bij het kiezen van een laag krijgt de gebruiker direct feedback over de consequenties van zijn of haar keuze. Ook biedt het mechanisme een gelaagde vorm van informatie aan de gebruiker: de website zelf heeft een aantal iconen en een knop die aangeven hoe het met de cookies geregeld is, door op de knop te drukken krijgt de gebruiker een summier overzicht van het privacybeleid, en daarin kan de gebruiker doorklikken naar een uitgebreide omschrijving van dit beleid.

Cookie controls van de BT website http://www.bt.co

2.4.4 Persoonsgegevensdashboard

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Een persoonsgegevensdashboard beoogt de transparantie over het gegevensbeheer voor de betrokkenen te vergroten.	*Een persoonsgegevensdashboard wordt beschikbaar gesteld bij of als onderdeel van de oplevering van een systeem.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Een persoonsgegevensdashboard heeft betrekking op alle gegevens die over een betrokkene in een bepaalde context worden verzameld en bewerkt.	*IT verantwoordelijke in samenspraak met de privacy officer / functionaris.*

Een persoonsgegevensdashboard is een online locatie waar een overzicht verkregen kan worden over de omgang met persoonlijke informatie. De gebruiker heeft online beschikking tot zijn persoonlijke data en kan controleren hoe data worden verwerkt. Bedrijven als Google en Microsoft gebruiken de persoonlijke gegevens van gebruikers voor reclamedoeleinden en hebben beide een persoonsgegevensdashboard ontwikkeld. Het dashboard van Microsoft heeft als doel de gebruiker een centrale locatie aan te bieden waar de gebruiker online persoonlijke informatie gerelateerd aan verschillende diensten van de organisatie kan bekijken en beheren. De gebruiker kan tot op zekere hoogte bepalen hoe Microsoft de persoonlijke data mag gebruiken.

Het persoonsgegevensdashboard van Google geeft een overzicht van de persoonsgegevens die aan het desbetreffende Google-account zijn gekoppeld. Het doel is om transparantie en controle te bieden aan de gebruiker, door middel van een overzicht van de persoonlijke gegevens gerelateerd aan Google producten (zoals Gmail, agenda, documenten, webgeschiedenis, alerts, Youtube, Picasa webalbums). Ook veel webwinkels maken gebruik van een persoonsgegevensdashboard om online inzicht te bieden in de aankoopgeschiedenis van klanten.

Voorbeeld: Midata

Het Britse ministerie van *Department for Business, Innovation & Skills* heeft een project genaamd “Midata”gelanceerd met als doel consumenten beter toegang te geven tot de elektronische persoonsgegevens die bedrijven over hen hebben. Dit kan bijvoorbeeld gaan om overzichten van eerdere aankopen. De wijze waarop dit wordt gerealiseerd is met behulp van wetgeving. Bedrijven die niet vrijwillig de elektronische persoonsgegevens vrijgeven kunnen middels de wet hiertoe gedwongen worden. In eerste instantie wordt echter gezocht naar vrijwillige deelname, waarbij het ministerie focust op drie sectoren: banken, mobiele telefonie aanbieders en energiebedrijven. Meer dan 20 bedrijven hebben zich al aangemeld voor deelname aan het Midata project, waaronder Visa, Mastercard, Three, Lloyds, RBS, British Gas en EDF Energy. Een voor de hand liggende manier waarop deze gegevens vrijgegeven kunnen worden is door het gebruik van een persoonsgegevensdashboard.

Meer lezen over deze case:
https://www.gov.uk/government/policies/providing-better-information-and-protection-for-consumers/supporting-pages/personal-data

2.4.5 Access logs

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Verantwoording door verwerker	*Tijdens verwerking en bij verantwoording achteraf*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Verzamelen, gebruik, bewerken, opslag en vernietigen persoonsgegevens	*IT-verantwoordelijke*

Een access log is een automatisch bijgehouden lijst die van alle verzoeken om toegang tot persoonsgegevens die in een bestand of op server staan. In zekere zin is de technologie dan ook vergelijkbaar met een zwarte doos in een vliegtuig: het stelt de beheerder in staat om terug te traceren wie tot welke data toegang heeft gehad, deze gewijzigd of gewist heeft. De lijst is

doorgaans chronologisch en bevat vaak kenmerken van de partij die het verzoek doet en van het bestand dat is opgevraagd.

De ruwe data die op de lijst staan, kunnen geanalyseerd worden door andere programma's. Analyse van access log files kan inzicht geven in zaken zoals: wie de data opvraagt of wijzigt, hoe vaak de data is opgevraagd, welke wijzigingen zijn aangebracht, of complexere gebruikspatronen. Gewoonlijk zijn access logs niet publiek toegankelijk. Ook toegang tot de log file wordt doorgaans gelogd. Access logs worden vaak gebruikt voor het beheer van computersystemen of websites, maar kunnen ook gebruikt worden voor privacydoeleinden. Zo kan er worden bijgehouden wie er toegang heeft of probeert te krijgen tot een bepaald bestand en of dit toegestaan is, waarmee mogelijkheden ontstaan voor het uitvoeren van controles achteraf en het verantwoording afleggen over de wijze waarop met persoonsgegevens wordt omgegaan. Access logs zijn wereldwijd zeer breed toegepast in allerlei verschillende systemen.

2.5 Zelfredzaamheid in privacy

Welke oplossingen stellen een burger of consument in staat om zelfstandig zijn of haar privacy te beschermen?

In tegenstelling tot de andere combinaties richt deze combinatie zich helemaal op de burger of consument, die zélf zijn of haar privacy wil beschermen. In het leveren van dergelijke oplossingen ligt mogelijk ook een kans voor bedrijven. Voor zelfredzaamheid in privacy zijn nu al verschillende hulpmiddelen beschikbaar, waarvan we hier een aantal *best technologies* bespreken. Allereerst is er een diversiteit aan tools die de gebruiker inzicht kunnen bieden in de wijze waarop met zijn of haar persoonsgegevens wordt omgegaan. Daarnaast beschikken de meeste moderne browsers over een 'private browsing' functionaliteit, en is er het Do Not Track initiatief. Meer geavanceerd is het gebruik van speciale proxy servers of onion routing technologie. Tot slot wordt ook gekeken naar de encryptie van opgeslagen data, bijvoorbeeld in de cloud.

2.5.1 Transparantietools

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Transparantietools dienen om het vertrouwen van betrokkenen in webdiensten te vergroten.	*Transparantietools kunnen door betrokkenen in alle stadia van een gegevensproces worden ingezet, afhankelijk van de mogelijkheden van de tool.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Transparantietools bieden de mogelijkheid om stromen van persoonsgegevens te volgen of daar gerichte acties op te ondernemen.	*Betrokkenen zijn zelf verantwoordelijk voor de inzet van deze tools.*

Transparantietools geven inzicht in de verwerking van persoonsgegevens door websites en bedrijven. Ruwweg kunnen twee typen instrumenten worden onderscheiden. Het eerste type geeft inzicht aan consumenten of gebruikers in hoe organisaties omgaan met persoonsgegevens. Het tweede type geeft inzicht aan consumenten of gebruikers in hoe zij zelf omgaan met hun persoonsgegevens. Daarnaast is er nog een onderscheid mogelijk tussen verschillende functionaliteiten. Er zijn softwarepakketten, web-based instrumenten, websites die informatie geven over de verwerking van persoonsgegevens en er zijn softwarepakketten die de privacy van de gebruiker waarborgen terwijl ze online zijn. Drie bekende transparantietools zijn Collusion, Ghostery en Do Not Track+.

Het doel van transparantiemechanismen is om het vertrouwen van consumenten en burgers in websites of bedrijven te verhogen doordat ze inzage krijgen in de verwerking van hun persoonsgegevens. Doelgroep zijn consumenten en internetgebruikers. Er is ook een groep transparantiemechanismen dat specifiek actief is op het gebied van medische gegevens.

2.5.2 Private browsing

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Data minimalisatie	*Tijdens gebruik browser*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Verzamelen van persoonsgegevens	*Gebruiker*

Vrijwel alle hedendaagse internet browsers bieden gebruikers de mogelijkheid tot 'private browsing', wat als doel heeft om het onmogelijk te maken voor gebruikers van dezelfde computer

om uit te vinden welke websites met de browser bezocht zijn, en om het onmogelijk te maken voor websites om uit te vinden of een bepaalde gebruiker ze eerder bezocht heeft. Om dit te realiseren zorgt de browser als deze in 'private browsing' mode staat dat de surfgeschiedenis, tijdelijke bestanden, cookies en dergelijke niet opgeslagen worden, of na het gebruik gewist worden.

In de browser Internet Explorer heet dit 'InPrivate Browsing', in Chrome heet het 'Incognito mode' en in Firefox en Safari heet de modus 'private browsing'. Deze modus wordt regelmatig gebruikt, al is er weinig zicht op de precieze gebruikscijfers of de redenen voor het gebruik van de modus. In een gebruikersonderzoek concludeerde Mozilla (aanbieder van de FireFox browser) dat 'private browsing' modus op verschillende momenten van de dag gebruikt wordt, met een opvallende piek rond lunchtijd.[76] Een mogelijke verklaring kan zijn dat gebruikers privé-internetgebruik op de werkcomputer tijdens lunchtijd in de 'private browsing' modus doen. Een ander onderzoek geeft aan dat 'private browsing' gebruikt wordt voor 18+ websites, online winkelen en het bezoeken van nieuws sites.[77]

De privacybescherming die een 'private browsing' modus aan gebruikers biedt is echter beperkt, en zeker geen garantie op privacy op het internet. Ten eerste is de communicatie tussen website en browser in principe te volgen door de internet service provider of de werkgever (als via een bedrijfsnetwerk tot internet toegang wordt verkregen). Ten tweede is het voor websites mogelijk om aan de hand van het IP adres en andere informatie computers (en daarmee gebruikers) te volgen zonder dat er gegevens zoals middels cookies op de computer van de gebruiker geplaatst worden. Tot slot blijkt ook de 'private browsing' mode zelf niet altijd even goed te werken en blijven op de computer zelf soms sporen van een 'private' sessie achter.

De 'private browsing' modus van moderne browsers biedt een beperkte vorm van privacybescherming aan vooral consumenten, die echter niet perfect is. Door bedrijven wordt 'private browsing', voor zover bekend, niet systematisch toegepast.

2.5.3 Do Not Track

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Do Not Track dient om de voorkeuren van de betrokkenen met betrekking tot het volgen van zijn/haar internetgedrag expliciet te maken.	*Do Not Track kan in een browser geïmplementeerd worden en kan dan door de betrokkene geactiveerd worden.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Do Not Track heeft betrekking op de praktijk van derde partijen om – vaak door het plaatsen van tracking cookies – gegevens over het internetgedrag van betrokkenen te verzamelen.	*De betrokkenen zijn zelf verantwoordelijk voor de implementatie van Do Not Track functionaliteit. Indien gewenst kan de implementatie door de IT-afdeling worden verzorgd.*

Do Not Track (DNT) is een technologie waarmee internetgebruikers aan kunnen geven dat ze niet gevolgd willen worden op het internet. In de praktijk betekent dat dat er geen tracking cookies geplaatst worden. Er is een standaard ontwikkeld door het World Wide Web Consortium (W3C).[78]

[76] Mozilla Blog of Metrics, 2010, Understanding Private Browsing
http://blog.mozilla.org/metrics/2010/08/23/understanding-private-browsing/

[77] Aggarwal, 2010, An Analysis of Private Browsing Modes in Modern Browsers
http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf

[78] W3C informatie over DoNotTrack: http://www.w3.org/TR/tracking-dnt

Op Stanford University is veel aan de ontwikkeling en randvoorwaarden van de technologie in het algemeen gedaan. Wanneer een gebruiker DNT heeft ingeschakeld, ontvangen aanbieders van web content hiervan bericht via de headerinformatie. De gebruiker geeft zo zijn wens aan en de aanbieder dient dat te respecteren door inderdaad geen tracking cookie te plaatsen.[79]

De technologie is beschikbaar voor ontwikkelaars en gebruikers. Enkele browsers hebben de technologie geïmplementeerd waardoor eenvoudig via de browserinstellingen de optie ingeschakeld kan worden. Enkele browsers hebben zelfs de optie standaard aangevinkt gezet.

Het beoogde voordeel van de technologie is dat gebruikers in één keer hun wensen kunnen instellen voor alle webdiensten met betrekking tot tracking cookies. Het concept is ontwikkeld, er is een standaard, en browseraanbieders hebben de technologie geïmplementeerd. De toepassing is daarmee wereldwijd beschikbaar. In de praktijk zijn er nog wel enkele kanttekeningen te plaatsen, met name omdat het van de aanbieders van web content afhangt of ze de wens van de gebruiker honoreren, wat (nog) geen gemeengoed is.

Voorbeeld: Do Not Track

Enkele jaren terug (2007) adviseerde de Amerikaanse *Federal Trade Commission* om gebruikers de mogelijkheid te geven een zwarte lijst op te stellen van bedrijven die geen toestemming kregen om persoonlijke informatie over de gebruikers te verzamelen. Dit leidde tot de gedachte om een Do Not Track optie in webbrowsers in te bouwen. Op dit moment bieden verschillende webbrowsers de DNT-functionaliteit aan. In principe kan een gebruiker kiezen uit drie opties: indien de DNT-optie op '0' staat, geeft dit aan dat de gebruiker instemt met het plaatsen van tracking cookies. Indien de DNT-optie op '1' staat, wil de gebruiker verschoont blijven van *tracking cookies*, en indien er geen waarde is ingevuld ('NULL') dan heft de gebruiker nog geen voorkeur uitgesproken. Er is geen sanctie indien een adverteerder of een andere organisatie de instelling van de DNT-optie negeert.

Verder lezen:

http://en.wikipedia.org/wiki/Do_Not_Track

2.5.4 Versleuteling van opgeslagen persoonsgegevens

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Verhinderen ongeautoriseerde toegang tot persoonsgegevens	*Bij opslaan en gebruik van persoonsgegevens*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Opslag en gebruik	*IT-verantwoordelijke, gebruiker*

Persoonsgegevens worden op een grote verscheidenheid aan plaatsen opgeslagen zoals op bedrijfsservers, op internet servers, op computers van personen of op USB-sticks. In veel gevallen zijn deze opgeslagen gegevens niet eenvoudig toegankelijk voor onbevoegden, bijvoorbeeld wanneer ze op een bedrijfsserver staan die fysiek en digitaal goed afgeschermd is van de

[79] Stanford/EFF werk is te zien op: http://donottrack.us

buitenwereld. In andere gevallen worden gegevens opgeslagen of vervoerd op media die veel kwetsbaarder zijn voor onbevoegde toegang, bijvoorbeeld door verlies van de drager (zoals een USB-stick, laptop of smartphone). In de praktijk is deze kwetsbaarheid voor verlies van een drager met persoonsgegevens een bron van lekken.

Een *best practice* die de risico's rond het lekken van opgeslagen persoonsgegevens sterk vermindert is encryptie van de opgeslagen gegevens. Zo kan een database die persoonsgegevens bevat versleuteld worden zodat alleen apparaten of personen die over de sleutel beschikken de gegevens kunnen lezen. Op soortgelijke wijze kan het bestandssysteem op een laptop of USB versleuteld worden zodat alleen de persoon die de sleutel heeft de bestanden kan lezen.

Encryptie van opgeslagen persoonsgegevens is een breed toegepaste en bewezen effectieve *best practice*, zoals het College Bescherming Persoonsgegevens ook aangeeft in haar nieuwe richtlijnen voor de beveiliging van persoonsgegevens.[80] De maatregel is ook uitgewerkt in standaarden zoals die van NEN-ISO.[81] Daarnaast zijn er veel *off-the-shelf* producten beschikbaar die encryptie van opgeslagen (persoons-)gegevens ondersteunen.

Voorbeeld: TrueCrypt

Een voorbeeld van een veelgebruikt programma om opgeslagen (persoons)gegevens te versleutelen is TrueCrypt, een open-source disk encryptie applicatie. De applicatie biedt de mogelijkheid tot zeer sterke encryptie die vrijwel niet te kraken is zonder het juiste wachtwoord te weten. Daarnaast is er functionaliteit zoals "hidden volume", wat inhoudt dat als de gebruiker gedwongen wordt een wachtwoord af te geven, deze een nep-wachtwoord kan afgeven wat geen toegang geeft tot de kritieke bestanden, maar tot een nep-schijf met onschuldige bestanden die als afleiding kunnen dienen. Een andere eigenschap is dat de versleutelde bestanden op zodanige wijze verborgen kunnen worden dat het niet aan te tonen is of een bestand een versleuteld archief is, of dat het willekeurige data is ("plausible deniability").

Meer lezen over TrueCrypt:
http://www.truecrypt.org/

2.5.5 Onion Routing

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Anonimisering van internetgebruik	*Tijdens gebruik internet*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Verzamelen en koppelen van persoonsgegevens	*Externe partij, gebruiker*

Onion Routing is een technische oplossing waarmee anoniem internetverkeer mogelijk wordt. Als een internetgebruiker van *onion routing* gebruik maakt is het voor een partij die berichten onderweg onderschept in principe niet mogelijk om te bepalen met wie de gebruiker communiceert.

[80] CBP - 2013 - Richtsnoeren beveiliging van persoonsgegevens
http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[81] NEN, 2007, Code voor informatiebeveiliging NEN-ISO/IEC 27002:2007 nl
http://www.nen.nl/NEN-Shop/Vakgebieden/ICT/ISO27001-Informatiebeveiliging/NENISOIEC-270022007-nl-1.htm

Internetverkeer van gebruikers wordt normaal gesproken langs een reeks servers geleid die het verkeer van de zender naar de ontvanger sturen. Om te bepalen waar een bericht heen moet, bevat deze gewoonlijk een *header* waarin de afzender en de ontvanger genoemd staan. Door deze *header* te lezen (bijvoorbeeld met *Deep Packet Inspection* technologie) kunnen servers waar het bericht langs komt bepalen wie met wie communiceert.

Een *onion routing* systeem leidt het internetverkeer van gebruikers door een willekeurig gekozen pad langs een aantal speciale servers. De berichten worden volledig onleesbaar gemaakt (inclusief header), middels encryptie. Bij elke server wordt een nieuwe encryptie 'schil' om het bericht toegevoegd (de naam *'onion'* verwijst naar deze 'schillen'). Elke server weet hierdoor slechts van welke server hij het bericht krijgt en naar welke volgende server hij het bericht moet sturen. Geen enkele server waar het bericht langs komt weet hoe de volledige route loopt van verzender naar ontvanger.[82]

Het *onion routing* concept is in 1995 in een project uitgewerkt, gefinancierd door de Amerikaanse *Office of Naval Research (ONR)* en het *Defense Advanced Research Projects Agency (DARPA)*.

Voorbeeld: Tor

In 2003 leidde vervolgonderzoek tot een implementatie in het zogenaamde 'Tor'-netwerk (*The onion routing*). De financiering van Tor is in 2004 door ONR en DARPA stopgezet, en overgenomen door de *Electronic Freedom Foundation*, een burgerrechtenbeweging voor de digitale wereld.

Het Tor netwerk is in de afgelopen jaren snel gegroeid, en bestaat inmiddels uit duizenden servers wereldwijd. Groepen gebruikers zijn onder andere individuen die Tor gebruiken voor sociaal gevoelige communicatie zoals chatrooms en forums voor slachtoffers van misbruik of mensen die leiden aan bepaalde ziekten, journalisten die met klokkenluiders en dissidenten communiceren, Niet-Gouvernementele Organisaties die hun werknemers vanuit het buitenland met het thuisfront laten communiceren, en bedrijven gebruiken het om bepaalde commercieel gevoelige communicatie te beveiligen voor afluisteraars.

Het Tor netwerk lijkt ook gebruikt te worden voor verschillende criminele activiteiten zoals handel in drugs en het verspreiden van kinderporno. Het Tor project geeft hierover zelf aan dat criminelen wel betere manieren hebben om hun activiteiten te verbergen, en dat Tor bedoeld is om 'gewone burgers de mogelijkheden tot anonimiteit te bieden die criminelen nu al hebben.'

Meer lezen over Tor:
http://www.onion-router.net/

[82] Roger Dingledine et al, 2003, Tor: The Second-Generation Onion Router
http://www.nrl.navy.mil/chacs/pubs/03-1221.1-2602.pdf

2.5.6 Proxy servers

Waartoe dient de oplossing?	**Wanneer** wordt de oplossing gebruikt?
Proxy servers bieden de mogelijkheid om tot op zekere hoogte anoniem van het internet gebruik te maken.	*Proxy servers worden gebruikt om informatiestromen en identiteiten te maskeren.*
Waarop heeft de oplossing betrekking?	**Wie** is verantwoordelijk?
Proxy servers vormen een anonieme toegangspoort tot internet.	*Betrokkenen zijn zelf verantwoordelijk voor het al dan niet benutten van proxy servers.*

Een *proxy server* is een server die als een doorgeefluik tussen de computer van de gebruiker en het internet fungeert. Voor andere servers en computers waar de gebruiker via een versleutelde verbinding mee communiceert is alleen de server zichtbaar en niet de computer van de gebruiker. Een *proxy server* is een doorgeefluik voor het internetverkeer van een groot aantal verschillende gebruikers, en hierdoor is het niet langer mogelijk om internetverkeer te herleiden tot een specifieke gebruiker aan de hand van het internetadres van de computer. Een *proxy server* biedt daarmee geen volledige bescherming: niet versleutelde communicatie kan nog steeds onderschept worden, en de gebruiker kan zelf identificerende sporen nalaten bij internetgebruik.[83]

Proxy servers worden ook voor andere doeleinden gebruikt dan privacybescherming, zoals het monitoren en filteren van internetverkeer om bepaalde ongewenste websites te blokkeren of het 'cachen' van internetverkeer om herhaalde verzoeken om dezelfde informatie sneller te laten verlopen. Dergelijke proxy servers worden veel gebruikt door bijvoorbeeld bedrijven of scholen. Een *proxy server* die privacy beschermt heeft dan ook een specifieke combinatie die anders is dan bijvoorbeeld een *proxy server* die het internetverkeer van gebruikers filtert.

Voor individuele gebruikers en organisaties zijn diensten beschikbaar van veel verschillende aanbieders die toegang tot een privacy-beschermende *proxy server* tegen een bepaalde vergoeding aanbieden. Hierbij speelt vertrouwen een centrale rol: de afnemer moet vertrouwen dat de dienstaanbieder de *proxy server* zodanig geconfigureerd heeft dat het verkeer niet gemonitord en geregistreerd wordt. *Proxy servers* met als doel privacybescherming worden wereldwijd veel gebruikt, bijvoorbeeld om privé te kunnen browsen, om restricties op internetdiensten te omzeilen, maar ook om als journalist bronnen te beschermen.

Proxy servers worden ook gebruikt als onderdeel van *onion routing*, waarin een reeks van *proxy servers*, gecombineerd met encryptietechnologie, de anonimiteit van gebruikers ook garanderen als één van de *proxy servers* het verkeer zou monitoren.

[83] Zie voor een inleiding tot proxy servers voor privacy: TechRepublic: The basics of using a proxy server for privacy and security
http://www.techrepublic.com/blog/security/the-basics-of-using-a-proxy-server-for-privacy-and-security/8762

Voorbeeld: Hide My Ass

Een voorbeeld van een proxy dienst is “Hide My Ass”, die een gratis en een betaalde variant aanbiedt. Hide My Ass biedt verschillende functionaliteiten aan, van eenvoudige proxy tot het beveiligd binnenhalen van bestanden. De dienst houdt lijsten bij van proxy servers die gebruikt kunnen worden waardoor gebruikers makkelijk kunnen switchen van de ene proxy server naar de andere. Daarnaast biedt het beveiligde email accounts aan en andere vormen van privacy software.

Meer lezen:

http://www.hidemyass.com/

3 Conclusie

Deze inventarisatie van *best technologies* en *best practices* voor het realiseren van privacybescherming laat een grote verscheidenheid aan oplossingen zien. Sommige oplossingen zijn technologisch van aard, sommige juist organisatorisch. Sommige richten zich op het ontwerpen van diensten, andere op het regelen van afspraken over de omgang met persoonsgegevens over verschillende diensten heen. De lijst met oplossingen toont welke kansen er voor bedrijven zijn: kansen om door het toepassen van innovatieve oplossingen effectievere en efficiëntere privacybescherming te realiseren én kansen om zelf innovatieve oplossingen te ontwikkelen en aan te bieden.

Zoals in de inleiding al genoemd: tussen het zich bewezen hebben in de praktijk en kansen bieden op innovatie zit een spanningsveld. Voor de doeleinden van het Actieplan Privacy zijn juist die *best technologies* en *best practices* interessant die zich midden in dit spanningsveld bevinden: een technologie of dienst heeft zich al bewezen in een beperkte omgeving, terwijl de potentie voor grotere uitrol zichtbaar is maar nog niet gerealiseerd. Tijdens de volgende activiteiten binnen het Actieplan Privacy worden in een tweetal consultatierondes met bedrijven, organisaties uit de publieke sector en wetenschappers die *best technologies* en *best practices* die zich op dit grensvlak bevinden geïdentificeerd en wordt vervolgens besproken hoe deze tot verder toepassing gebracht kunnen worden. Een geselecteerd aantal van deze *best technologies* en *best practices* wordt vervolgens verder uitgewerkt. De resulterende *best innovations* worden in december 2014 gepresenteerd.