Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2017 R10680

RESPECT4U

Datum	6 juni 2017
Auteur(s)	Marc van Lieshout, Somayeh Djafari, Petra Vermeulen
Aantal pagina's	24
Projectnummer	060.24401

Inhoudsopgave

1 Inleiding

Het belang van privacy voor organisaties neemt toe. Verschillende ontwikkelingen dragen hieraan bij. Op de eerste plaats is dit de enorme groei aan – vrijelijk verkrijgbare – gegevens. Veel van deze gegevens zijn tot personen te herleiden en hebben daarmee impact op de privacy van individuen. Ten tweede, veel nieuwe diensten zijn gebaseerd op de verwerking van (persoonlijke) gegevens. Deze nieuwe diensten leiden tot geheel nieuwe sectoren van economische activiteit, waarin organisaties elkaar beconcurreren op de aandacht van de consument. Ten derde vergroot de opkomst van het internet der dingen de ontwikkeling van nieuwe persoonlijke dienstverlening. Tot slot, kunstmatige intelligentie en lerende machines zijn in staat verbanden tussen gegevens te leggen die ‘met de hand’ nooit zouden zijn gevonden. Dat brengt nieuwe kansen mee, maar ook nieuwe zorgen. Nieuwe vormen van discriminatie, stigmatisering, uitsluiting en onheuse bejegening liggen op de loer, ook als dit geenszins de bedoeling is.

De Europese Unie heeft in april 2016 de opvolger van de Dataprotectie Richtlijn (95/46/EU) aangenomen. Deze Richtlijn dateert uit 1995 en was gebaseerd op de omgang met gegevens zoals die plaatsvond in het pre-internet tijdperk. Zijn opvolger, de Algemene Verordening Gegevensbescherming (AVG) biedt vanaf 25 mei 2018 formeel het wettelijk kader rond de bescherming van personen in relatie tot de verwerking van hun gegevens (zoals de wet voluit heet). Als Verordening geldt de AVG in alle lidstaten op gelijke wijze. De AVG geeft de betrokkenen (de personen over wie gegevens worden verwerkt) bepaalde rechten en legt de verwerkingsverantwoordelijken en de verwerkers (partijen die voor deze verantwoordelijken de gegevens verwerken) bepaalde plichten op. Evenals de Richtlijn geeft de Verordening vooral voorwaarden voor een verantwoorde omgang met persoonsgegevens maar legt het niet in detail vast wat de minimumvoorwaarden zijn voor die verantwoorde omgang. Meer nog dan de Richtlijn geeft de Verordening organisaties de gelegenheid zelf de noodzakelijke maatregelen te treffen voor een verantwoorde verwerking van persoonsgegevens. In ruil daarvoor stelt hij wel hogere eisen aan de verantwoording van de handelswijze. Belangrijk onderdeel daarvan is het daadwerkelijk kunnen tonen dat de organisatie zich realiseert dat ze actie moet ondernemen en dat ze ook passende beschermende maatregelen heeft getroffen. In bepaalde gevallen is ze verplicht een dataprotectie impact assessment uit te voeren om op voorhand de privacyrisico’s in kaart te brengen. Iedere organisatie dient zich rekenschap te geven van de mogelijkheden van dataprotectie *by default* en dataprotectie *by design*. We komen daar nog uitvoerig op terug. Betrokkenen kunnen een uitgebreider pakket aan rechten laten gelden dan voorheen, waaronder het recht op een elektronische kopie van hun gegevens, het recht om hun gegevens mee te mogen nemen naar een andere dienstverlener en het recht op vergetelheid. Die rechten zijn op hun beurt weer gebonden aan bepaalde voorwaarden van redelijkheid.

Het Privacy & Identity lab, een samenwerking tussen drie Nederlandse kennisinstellingen, Radboud Universiteit, Tilburg University en TNO draagt bij aan de ontwikkeling van privacyrespecterende maatregelen. De uitdagingen die in het voorgaande kort aan de orde zijn gesteld, vormen de grondslag voor de ontwikkeling van innovatieve en toegesneden oplossingen. TNO, met zijn focus op

toepassingsgerichte kennis, heeft de uitdagingen die de AVG stelt aan organisaties aangegrepen voor de ontwikkeling van een privacyraamwerk, RESPECT4U genaamd. Dit raamwerk biedt een aantal handvatten om privacy in de bedrijfsvoering van organisaties te integreren. Het raamwerk kiest daarbij voor een positieve insteek, waarbij het inspeelt op de geschetste trends om privacy ook als businesswaarde te benoemen.

Het RESPECT4U raamwerk is op de AVG gebaseerd. Het beschermen van personen in relatie tot de verwerking van hun gegevens vraagt echter om meer dan het respecteren van de wettelijke regels. Het vraagt om een omvattende benadering die juridische, technische en organisatorische aspecten integreert. Gegevens moeten veilig verwerkt worden, privacyrisico's moeten tijdig onderkend worden, de gehele organisatie moet betrokken zijn bij de concreet te maken verantwoording voor de handelswijzen. De claim van RESPECT4U is dat de investeringen in deze maatregelen winst voor de organisatie opleveren: door een betere beheersing van de gegevensstromen ontstaan efficiëntievoordelen, door een adequate bescherming worden andere beveiligingskosten vermeden, door transparant te zijn over handelswijzen en doeleinden van de gegevensverwerking vergroot een organisatie de vertrouwensrelatie met de klant.

2 Missie en visie van RESPECT4U

2.1 Missie

RESPECT4U onderschrijft dat mensen kunnen handelen als vrije en autonome individuen en dat ze beschermd worden tegen onredelijke beperkingen bij de vorming van hun eigen identiteit.[1] Deze omschrijving van privacy is er een uit vele. Wel is het een omschrijving die verschillende aspecten benadrukt die wij van belang achten in de hedendaagse 'datasamenleving'. Autonomie en vrijheid vormen de kern van een democratische samenleving. Een samenleving die burgers in staat stelt een leven te leiden volgens hun eigen normen en waarden waarbij ze maatschappelijke normen en regelingen, die eveneens door een democratisch proces zijn vastgesteld, respecteren. Een samenleving waarin de overheid zich tot doel stelt om zich waar mogelijk te onthouden van bemoeienis met de levens van burgers (klassieke grondrechten) en tegelijkertijd mogelijkheden creëert voor burgers om zich te ontwikkelen (sociale grondrechten). In de hedendaagse wereld waar grenzen in fysieke en virtuele zin verdwijnen zijn deze rollen en verantwoordelijkheden minder vanzelfsprekend en moet de afbakening tussen private en publieke ruimtes opnieuw doordacht worden. De zich vormende data-economie – waarin gegevens de grondstof, het halffabrikaat en het eindproduct van economische transacties zijn – vraagt om nieuwe regels die tegemoetkomen aan de geschetste democratische uitgangspunten en tegelijkertijd de mogelijke voordelen van de nieuwe dienstverlening ondersteunen.

We beschouwen privacy daarmee niet alleen als een individuele en persoonlijke waarde maar ook als een gemeenschappelijke en maatschappelijke waarde. De toenemende verwevenheid tussen online en offline dienstverlening en de vermenging tussen dienstverlening in de fysieke en de virtuele wereld bieden geweldige maatschappelijke kansen op betere zorg, beter verkeer en vervoer, beter onderwijs, betere benutting van schaarse grondstoffen enz. In toenemende mate is de mens niet alleen de afnemer van een product maar ook een van de samenstellende onderdelen. Dat geeft het individu ook een bijzondere status in de onderhandelingen over de ontwikkeling van en de omgang met die nieuwe diensten. RESPECT4U wil maatschappelijk wenselijke ontwikkelingen en individuele waarborgen tegen onevenredige inbreuken op de privacy bij elkaar brengen door maatregelen te presenteren die organisaties helpen om op een verantwoorde manier (persoons-)gegevens te verwerken bij de ontwikkeling en het aanbod van nieuwe diensten.

We zullen deze missie volbrengen door:

- Ons sterk te maken voor een duidelijk en innovatief leiderschap dat de privacy van alle Europeanen ten goede komt.
- Excellentie na te streven in het ontwerp en de productie van processen, hulpmiddelen en instrumenten die organisaties ondersteunen bij het voldoen aan de vragen van hun klanten bij het realiseren van de hoogst mogelijke privacykwaliteitsstandaarden.

[1] P. Agre and M. Rotenberg, Technology and Privacy: The New Landscape, MIT Press, 1997

- Het beschikbaar stellen van onderwijsmateriaal van de hoogste kwaliteit aan publieke en private organisaties zodat zij kunnen beschikken over de beste kennis om gebruik te maken van de richtlijnen en principes die we via RESPECT4U beschikbaar stellen, dit alles in het licht van het bevorderen van vrije en autonome individuen en het verminderen van significante risico's voor de bescherming van personen in relatie tot de verwerking van hun gegevens, in het bijzonder waar dit online activiteiten betreft.
- Het verspreiden van onze kennis, ervaringen en bevindingen op een open en vrije manier zodat ieder die daar kennis van wil nemen dit kan zonder hinder te ondervinden van onnodige barrières.

2.2 Visie

Europeanen hebben altijd waarde gehecht aan hun privacy. De individuele en maatschappelijke waarden die belichaamd worden door privacy ondersteunen het Europese ideaal van vrije en verantwoorde burgers. Over de jaren heen zijn deze waarden onderdeel geworden van een Europese waarborging via specifieke regelgeving. In de moderne tijd heeft er bescherming bestaan tegen het onrechtmatig binnentreden van andermans huis en het lezen van andermans brieven. Later zijn daar beschermende maatregelen tegen nieuwe communicatievormen bij gekomen, zoals bescherming tegen het afluisteren van de telefoon, het binnendringen in de computer en de afscherming van email.

Het is evenwel het Amerika van de negentiende eeuw dat de basis vormde voor het moderne recht op privacy. In een beroemd artikel in 1890 waren het de Amerikaanse advocaat Samuel Warren en rechter Louis Brandeis die het recht om met rust gelaten te worden ('the right to be let alone') van een stevige basis voorzagen. Deze benadering is in 1948 neergelegd in de Universele Verklaring van de Rechten van de Mens die stelt dat niemand onderworpen zal worden aan willekeurige inmenging in zijn privéaangelegenheden, gezinsleven, tehuis of briefwisseling. Deze rechten zijn inmiddels ook verankerd in het Europese Handvest van Grondrechten. De rechten zijn breder dan alleen betreffende gegevens over een persoon. Maar de vertaling naar gegevens kan gemaakt worden, zoals ook het Europese Handvest doet. Wij sluiten hier graag bij aan, temeer omdat dit recht kan leiden tot positieve benutting van gegevens. Iedereen die er zeker van kan zijn dat zijn of haar gegevens niet misbruikt zullen worden zal zich vrij voelen om in te gaan op een aangeboden dienstverlening die gebruik maakt van (persoonlijke) gegevens.

De hedendaagse samenleving maakt privacy belangrijker dan ooit. Het internet heeft geleid tot nieuwe commerciële relaties tussen klanten en bedrijven, tussen nieuwe vormen van publieke dienstverlening met een sterk persoonlijk accent. Veel van deze innovaties zijn mogelijk door een slimme en geavanceerde benutting van persoonlijke gegevens. Dit verplicht ons om te doen wat we vaker hebben gedaan: ervoor zorgen dat de waarde die we hechten aan privacy terug te vinden is in de technologieën en de omstandigheden van deze tijd.

2.3 4U

We hebben al aangegeven dat privacy niet alleen een atomistische en individuele waarde is maar ook een gemeenschappelijke en maatschappelijke dimensie heeft. In de toevoeging ‘4U’ hebben we die verschillende dimensies bij elkaar willen brengen. Eén U betreft het individu, U, wiens claim op privacy onweersproken is. Twee U’s verwijzen naar de relatie die individuen onderling kunnen hebben, een relatie die verwijst naar de intieme sfeer van het gezinsleven en goede vrienden. Drie U’s is de groep (‘three is a crowd’), de menigte die een samenstel is van bekenden en onbekenden. De menigte ook waarin U er zich van bewust is dat er geen absolute controle mogelijk is over wat er over U bekend is en rondgaat. Vier U’s, tot slot, is de groep van groepen, de samenleving, waar normen en regels bijdragen aan het handhaven van democratische principes als rechtvaardigheid, eerlijkheid en gelijke behandeling. RESPECT4U beoogt alle vier de sferen te bedienen door een afgewogen stelsel van maatregelen die ertoe bijdragen dat de privacy van personen, binnen de privésfeer, binnen relaties, binnen gekende en ongekende groepen en binnen de samenleving gerespecteerd wordt.

3 RESPECT4U

Figuur 1: Het RESPECT4U raamwerk

Figuur 1 toont in één blik de verschillende dimensies van het RESPECT4U raamwerk. Ieder van de letters correspondeert met een specifiek perspectief op de uitdagingen die voorliggen.

- Het begint met *Responsible*, de verantwoorde omgang met persoonsgegevens. Dit is gericht op het demonstreren van hoe deze verantwoordelijkheid in concreto wordt ingevuld.
- *Empowerment* geeft betrokkenen instrumenten om invloed uit te kunnen oefenen op de verwerking van hun gegevens.
- *Secure* betekent dat een organisatie maatregelen heeft getroffen die de veilige opslag van gegevens, de veilige toegang tot gegevens en de veilige verwerking van gegevens garanderen.
- *Pro-active* houdt in dat een organisatie tijdig stappen heeft gezet om privacyrisico's op te sporen en door inzet van de juiste maatregelen deze risico's aanpakt.
- *Ethical* verwijst naar bewustzijn met betrekking tot onvoorziene en ongewenste gevolgen van de verwerking van gegevens.
- *Cost-benefit analysis* maakt het mogelijk kosten én baten van de maatregelen naast elkaar te zetten.
- *Transparent*, tot slot, verwijst naar transparantie in de toebedeling van rollen en verantwoordelijkheden voor de verwerking van gegevens, en transparantie ten aanzien van doel en middelen van de gegevensverwerking.

4 Responsible

4.1 Achtergrond

De data-economie vormt een belangrijke pijler onder de hedendaagse samenleving. Gegevens van personen zijn onderdeel van een breed palet aan diensten en producten. Deze diensten komen tegemoet aan maatschappelijke vragen rond de zorg, energie, mobiliteit en het onderwijs en bieden burgers ongekende mogelijkheden om met elkaar in contact te treden.

De keerzijde van deze ontwikkeling is het verlies van controle over wat er met iemands gegevens gebeurt en een mogelijke inbreuk op de persoonlijke levenssfeer. Dit kan een verstarrend effect hebben op hoe mensen zich gedragen en hoe ze zich willen uiten. Het kan leiden tot onheuse bejegening van individuen en tot ongewenste vormen van discriminatie, stigmatisering en uitsluiting. Om deze mogelijke dreigingen het hoofd te bieden zijn organisaties nodig die bereid zijn verantwoording af te leggen voor hun handelswijze. Een verantwoorde omgang met persoonsgegevens wordt dan een hoeksteen om vertrouwen te verkrijgen en te behouden.

4.2 Uitwerking

Er is een beweging gaande waarbij organisaties zich niet alleen meer laten leiden door een focus op zo efficiënt, goedkoop en snel mogelijke productie en dienstverlening maar oog krijgen voor waarden als duurzaam, veilig, inclusief en respectvol. We verwachten dat organisaties die zich op deze laatste verzameling van waarden richten het langer en beter zullen volhouden dan de groep die vooral met de eerste soort waarden bezig is. We verwachten ook dat deze eerste groep organisaties bereid is om zichtbaar te maken hoe ze hun verantwoordelijkheid invullen.

4.3 Maatregelen

In relatie tot de verwerking van persoonsgegevens biedt de AVG een aantal handreikingen: het instellen van een data protectie officer, de aanvaarding van een Gedragscode, de introductie van certificeringsschema's. Daarnaast is te denken aan het opnemen van privacy in het jaarverslag, het uitvoeren van een benchmark die zichtbaar maakt hoe goed een organisatie het doet, het instellen van een klantenpanel, het aannemen van een privacystrategie die leidt tot een volwassen benadering van privacy binnen alle onderdelen van de organisatie.

Kader 1: Persoonlijke gegevens

De Algemene Verordening Gegevensbescherming heeft alleen betrekking op gegevens die natuurlijke personen betreffen. Het begrip ‘persoonsgegeven’ is breed opgevat: ieder gegeven dat direct of indirect kan leiden tot de identificatie van een natuurlijke persoon wordt beschouwd als een persoonsgegeven. Een naam is een gegeven dat direct kan leiden tot de identificatie van een natuurlijk persoon. Maar ook een kentekennummer en een IP-adres zijn persoonsgegevens! Door het kentekennummer of het IP-adres is het in principe mogelijk om een specifieke natuurlijke persoon te identificeren. Daarmee vallen ook deze gegevens onder de reikwijdte van de AVG.

5 Empowerment

5.1 Achtergrond

In onze hoedanigheid als burgers en als klanten delen we onze gegevens zonder dat we precies weten wat er met deze gegevens gebeurt. Het feit dat dit in wet- en regelgeving is vastgelegd, biedt in de praktijk weinig concrete handvatten. Onderzoek onder burgers en klanten stelt een aantal zorgen onomstotelijk vast: mensen zijn bezorgd om een potentiële inbreuk op hun privacy, mensen zouden meer controle over hun eigen gegevens willen en mensen zijn terughoudend als het om commerciële benutting van eerder verstrekte gegevens gaat.[2] Deze zorgen kunnen ten koste gaan van de bereidheid om gegevens te delen. Het toerusten van burgers en klanten met instrumenten die het mogelijk maken inzage te hebben in wat er met hun gegevens gebeurt en hier ook een zekere mate van controle over te kunnen uitoefenen draagt ertoe bij dat burgers en consumenten bereidheid blijven om gegevens te delen voor diensten die hen en anderen tot voordeel strekken.

5.2 Uitwerking

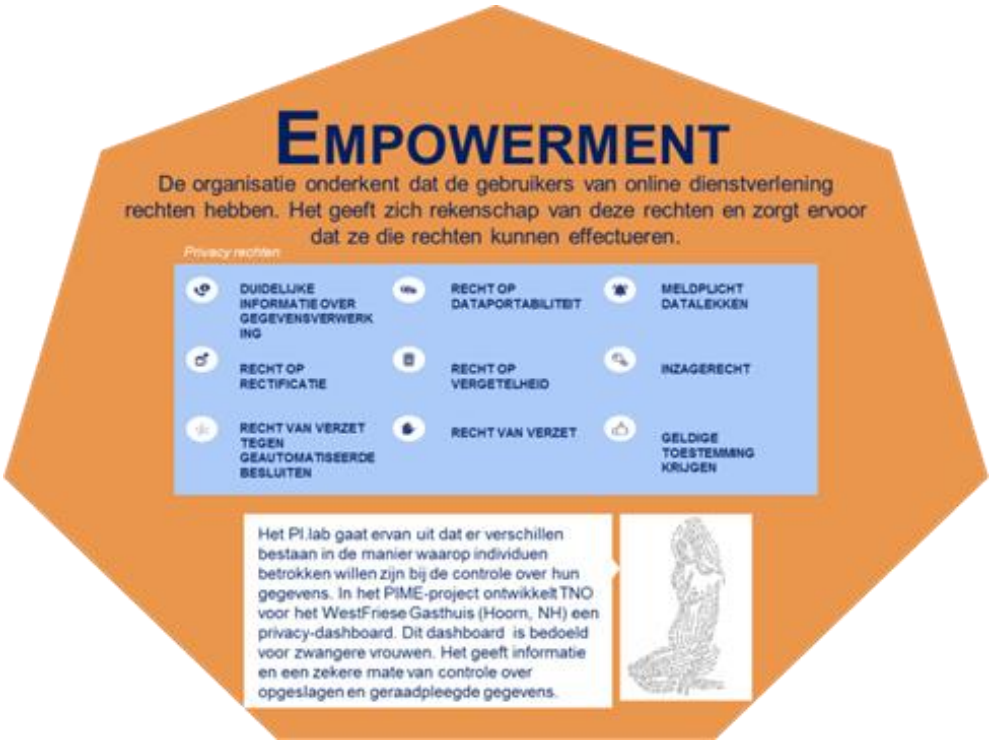
Empowerment is een belangrijke stap van organisaties om respectvol met de privacy van hun klanten om te gaan. Het erkent dat de betrokkenen een fundamentele rol spelen in de interactie met de organisatie en hier ook rechten aan kunnen ontlenen. Er is echter geen ‘one size fits all’ benadering in hoe burgers en klanten toegerust kunnen worden: sommigen willen over alles geïnformeerd worden en willen ook zoveel mogelijk controle uit kunnen oefenen, anderen vinden het prima als ze ervan op aan kunnen dat het goed geregeld is. Uitgangspunt is ook hier de verzameling aan rechten die de AVG aan de betrokkenen toekent. Door klanten en burgers de instrumenten te geven om betrokken te zijn op de manier die het best aansluit op hun behoeften respecteren organisaties de autonomie van deze individuen en werken ze aan vertrouwen.

5.3 Maatregelen

Een belangrijke maatregel is het instellen van een zogenaamd privacy dashboard. Zo’n dashboard komt tegemoet aan verschillende doeleinden: het informeert de betrokkenen over wat er over hen verzameld en verwerkt wordt en voor welke doeleinden dit gebeurt; het geeft aan wat de wettelijke basis is waarop dit gebeurt (de grondslag), en het geeft aan hoe de organisatie de verwerking van gegevens intern georganiseerd heeft. Een dashboard kan daarnaast de betrokkenen een zekere mate van controle geven over wat de organisatie mag doen met hun gegevens. Zo moet een betrokkene in staat zijn om een gegeven toestemming te allen tijde weer in te kunnen trekken. Ook kunnen betrokkenen in bepaalde gevallen bezwaar aantekenen tegen de verwerking van hun gegevens. Ook hebben betrokkenen het recht om onjuiste, incomplete of niet ter zake doende gegevens te corrigeren dan wel te laten verwijderen, kunnen ze vragen om hun gegevens over te dragen aan een andere dienstverlener en kunnen ze een recht op vergetelheid uitoefenen. Ze kunnen protest aantekenen tegen een automatisch genomen besluit, tegen automatisch opgestelde profielen en ze kunnen vragen wat de logica achter

[2] Referenties toevoegen

de besluitvorming is geweest (bijvoorbeeld: hoe komt het dat ze in een bepaald profiel zijn ingedeeld?). Veel van deze rechten zijn afhankelijk van de specifieke situatie. In een dashboard kan dit worden aangegeven zodat de betrokkenen weten waar ze aan toe zijn (en de organisatie ook).



Kader 2: Verwerken van gegevens

De AVG heeft betrekking op de verwerking van persoonsgegevens. Het begrip ‘verwerking’ moet breed opgevat worden. Het omvat alle mogelijke handelingen die met gegevens verricht kunnen worden, zoals verzameling, opslag, bewerking, verrijking, verspreiding, archivering, verwijdering, vernietiging.

6 Secure

6.1 Achtergrond

De veilige omgang met gegevens is een belangrijke performance indicator voor organisaties. Datalekken van welke aard dan ook leiden tot negatieve beeldvorming en flinke boetes. Een aantoonbaar veilige verwerking van persoonsgegevens draagt bij aan het vergroten van de betrouwbaarheid van de organisatie

6.2 Uitwerking

De veilige omgang met gegevens bestaat uit drie onderdelen: het beveiligen van de gegevens, het beveiligen van de toegang tot de gegevens, en het beveiligen van de verwerking van de gegevens. De AVG stelt hoge eisen aan de beveiliging. Dit noodzaakt tot het treffen van de juiste technische én organisatorische maatregelen binnen een organisatie. Op dit gebied vindt veel innovatie plaats. Over de tijd zullen deze innovaties hun weg vinden en bijdragen aan een verzekerde beveiliging op alle drie de fronten.

6.3 Maatregelen

Voor de veilige opslag en uitwisseling van gegevens zijn verschillende versleutelingstechnieken voorhanden. Hashing, pseudonimisering, gebruik van versleuteling, benutting van Trusted Third Parties voor gegevens- en sleutelbeheer behoort tot het standaardrepertoire. Daarnaast wordt gewerkt aan innovatieve benaderingen zoals secure multi-party computation, homomorfe encryptie en polymorfe encryptie en pseudonimisering. Deze technieken zijn vanuit cryptografisch oogpunt en uit een oogpunt van veilig gegevensbeheer veelbelovend maar zijn nog niet voldoende marktrijp om ‘off-the-shelf’ verkocht te worden. Homomorfe encryptie richt zich op de analyse van versleutelde gegevens zonder dat de gegevens vrijgegeven hoeven te worden. Secure multi-party computation maakt het mogelijk om met meer partijen op een veilige manier gegevens te verwerken. Polymorfe encryptie en pseudonimisering is hier ook een voorbeeld van met eigen kenmerken. Geavanceerde sleutelbeheersystemen zijn in ontwikkeling, en leiden tot gepersonaliseerde gegevenskluizen. Op attributen gebaseerde certificaten geven alleen de hoogst noodzakelijke gegevens vrij voor een transactie. De technische maatregelen vragen om een toegesneden organisatorische inbedding om tot optimaal resultaat te leiden. Tot slot: ook op het vlak van de identificatie van personen en het authentiseren van personen voor het mogen verrichten van bepaalde verwerkingshandelingen vinden nieuwe ontwikkelingen plaats, die bijvoorbeeld gebruik maken van biometrische kenmerken.

Kader 3: Doel en legitieme grondslag

Iedere verwerking van persoonsgegevens behoeft een legitiem doel en een legitieme grondslag. Het doel moet welgekozen zijn, het moet voldoende specifiek zijn en passend bij wat verwacht mag worden bij de organisatie of instantie die de persoonsgegevens voor dit doel wil verwerken. Het doel mag niet strijdig zijn met de wet. Als grondslag voor de gegevensverwerking staan zes mogelijkheden open:

(a) de expliciete, vrij gegeven en geïnformeerde toestemming van de betrokkene;
(b) het nakomen van een contract;
(c) een wettelijke verplichting;
(d) het vitale belang van de betrokkene;
(e) een publiek belang;
(f) het gerechtvaardigd belang van de verwerkingsverantwoordelijke.

Als gegevens voor een ander doel verwerkt gaan worden dan oorspronkelijk aangegeven moet opnieuw de rechtmatigheid van het doel bepaald worden en is een nieuwe grondslag nodig. Uitzondering hierop is het verrichten van wetenschappelijk onderzoek. Dit wordt gezien als ‘niet onverenigbaar met het oorspronkelijke doel’. De reden hiervoor is de veronderstelling dat wetenschappelijk onderzoek in de regel geen impact op de privacy van de betrokkenen heeft.

7 Pro-active

7.1 Achtergrond

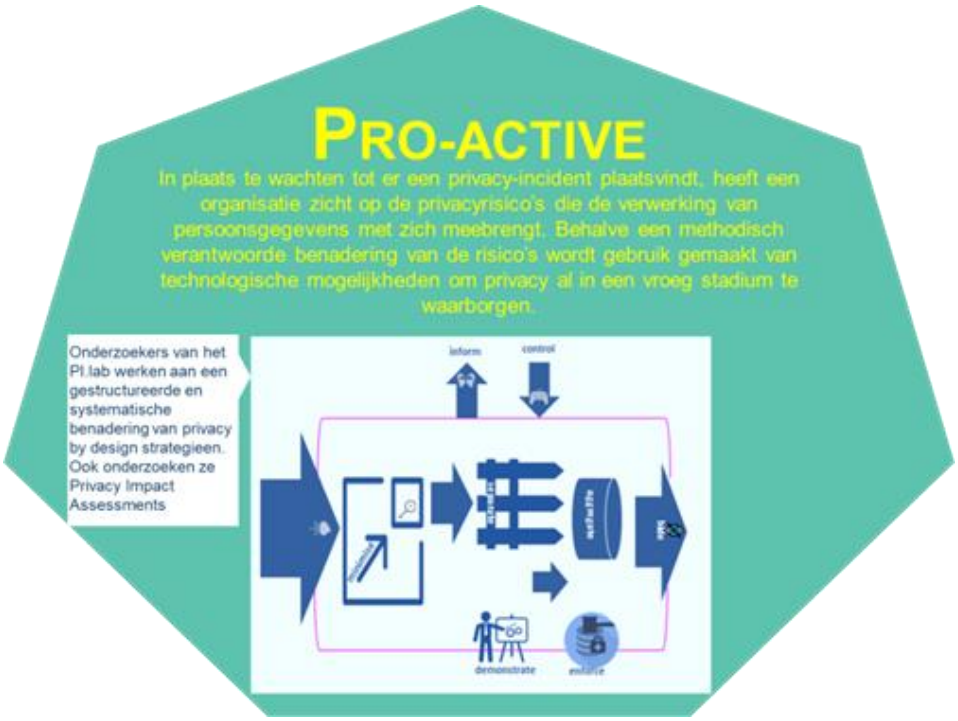
“An ounce of prevention is worth a pound of cure.” Deze uitspraak van Benjamin Franklin is niet alleen van toepassing in de fysieke wereld maar ook in de virtuele. Een inschatting van de privacyrisico’s van een nieuw systeem maakt het mogelijk om gepaste maatregelen te nemen voordat het systeem in gebruik wordt genomen. Dat vraagt om *data protection by design*, het nadenken over de manier waarop privacy van meet af aan in het systeemontwerp kan worden geïntegreerd, en het nadenken over *data protection by default*, het zodanig instellen van systeemparameters dat de privacy automatisch het best gediend is. Door de inschatting van privacyrisico’s en door een goede ontwerpbenadering voorkomt een organisatie negatieve privacygevolgen voor de betrokkenen, waardoor ook imago- en reputatieschade (en boetes) voor de organisaties vermeden worden.

7.2 Uitwerking

Een proactieve houding betekent een systematische en gestructureerde benadering van de privacyrisico’s van een voorgenomen gegevensverwerking, inzicht in de maturiteit van de organisatie om deze risico’s aan te pakken en de inzet van de juiste maatregelen om de risico’s te verkleinen of in hun geheel weg te nemen.

7.3 Maatregelen

De AVG stelt een *Data protection impact assessment* verplicht voor bepaalde typen verwerkingen. Deze DPIAs kennen nog geen geaccepteerde standaard. Wel zijn er verschillende modelbenaderingen beschikbaar die op een specifieke situatie kunnen worden afgestemd. Van belang is de gerichtheid van de DPIA: die heeft betrekking op het in kaart brengen van de risico’s voor de betrokkenen. Het is dus geen inschatting van de aansprakelijkheden van een organisatie voor een eventueel falen van de organisatie. Voor de integratie van privacy in het systeemontwerp kan gebruik worden gemaakt van privacystrategieën en -patronen. Die strategieën richten zich op dataminimalisatie en beveiligde verwerking van gegevens mogelijkheden tot pseudonimisering en anonimisering van gegevens door segregatie van identificerende en niet-identificerende gegevens, door aggregatie van gegevens zodat individuele personen niet meer herleidbaar zijn. Ook geven ze aan hoe een organisatie een verantwoorde omgang met persoonsgegevens af kan dwingen en kan laten zien dat het een en ander goed georganiseerd heeft. Tot slot geeft het aanwijzingen die tot empowerment van de betrokkenen leiden.



Kader 4: Pseudonimisering en anonimisering

Als persoonsgegevens geanonimiseerd zijn, vallen ze niet meer onder de werking van de AVG. Het zijn dan immers geen gegevens meer die direct of indirect tot een persoon te herleiden zijn. Met de toenemende mogelijkheden om snel grote hoeveelheden gegevens te verwerken neemt echter ook de principiële herleidbaarheid van gegevens tot natuurlijke personen toe, zoals uit vele onderzoeken naar voren is gekomen. Dat betekent dat daadwerkelijke anonimisering in de praktijk lastig is geworden. De formele toetssteen is dat het onevenredig veel tijd en inzet van bronnen (geld, techniek) kost om de identiteit van een persoon te achterhalen. De Artikel 29 Werkgroep heeft in een Opinie aangegeven welke technieken ingezet kunnen worden om persoonsgegevens afdoende te anonimiseren (Opinie 4/2013).

In veel gevallen zal het meer in de rede liggen om te streven naar pseudonimisering, dat wil zeggen het vervangen van identificerende gegevens door een pseudoniem, zoals een willekeurig getal. Wettelijk gezien zijn gepseudonimiseerde gegevens nog steeds persoonsgegevens en vallen daarmee nog steeds onder de werking van de AVG. Pseudonimisering draagt aanzienlijk bij aan beveiliging van de verwerking van gegevens en wordt door de AVG dan ook aangehaald als een van de in te zetten technieken.

8 Ethical

8.1 Achtergrond

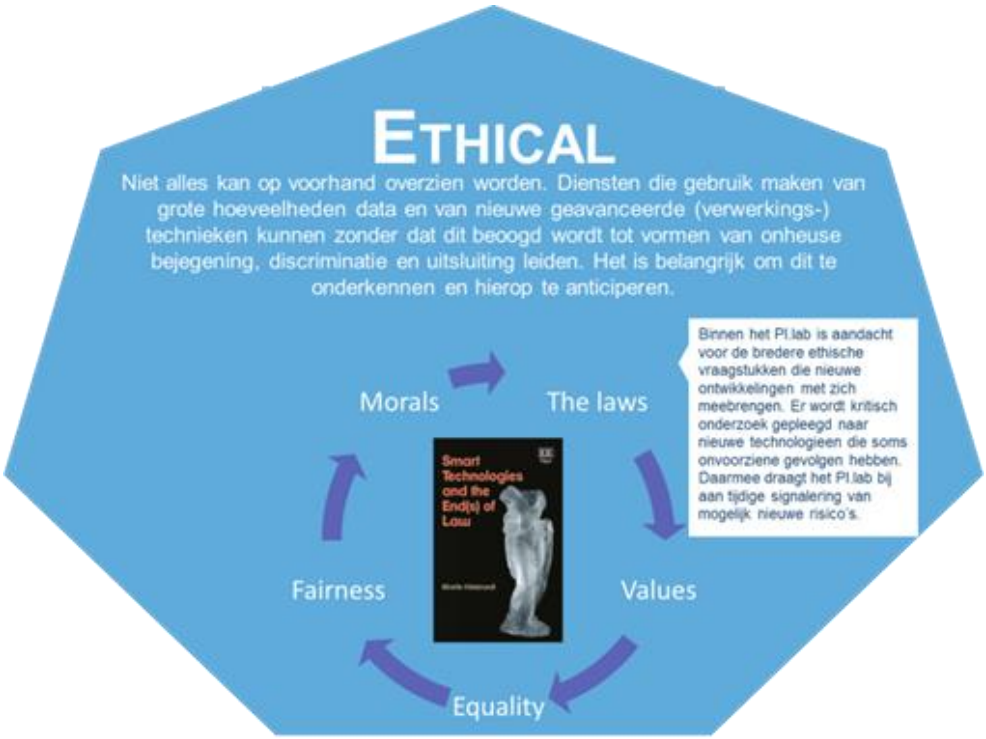
De door data gedreven innovaties hebben een impact op vele facetten van het dagelijks leven. Veel van de negatieve consequenties zijn op voorhand aan te geven en met gepaste maatregelen tegen te gaan. Dat is niet altijd mogelijk, door verschillende oorzaken. Gevolgen kunnen zich pas na verloop van tijd manifesteren, en niet altijd zijn alle gevolgen op voorhand te overzien. Er hoeft ook geen kwade opzet in het spel te zijn. Onvoorziene verwikkelingen kunnen nadelig uitpakken, zonder dat dit beoogd was. De toenemende inschakeling van AI en machine learning om grote hoeveelheden gegevens door te werken, op zoek naar verbanden en nieuwe kennis, leidt tot grotere risico's op discriminatie, onheuse bejegening, stigmatisering en uitsluiting. Dat kan bijvoorbeeld omdat onvoldoende zicht bestaat op de samenstelling van de gegevens die voor de analyse gebruikt worden, omdat de werking van de algoritmes niet meer te doorgronden is, of omdat keuzeprocessen door machines worden gedaan waar dit eerder door mensen plaatsvond. Dit leidt tot de noodzaak van een diepgaande reflectie op richting en aard van de ontwikkelingen. Dat perspectief is breder dan alleen privacy maar het blijft zich wel richten op de mogelijkheden om een vrij en autonoom leven te leiden.

8.2 Uitwerking

Een organisatie dient zich bewust te zijn van mogelijk nadelige gevolgen van haar handelen vanwege onvolmaaktheden in de verzamelde gegevens en onbekendheden in de gegevensverwerking. Het is moeilijk om hierover algemeen geldende uitspraken te doen. Het gebruik van niet-deterministische algoritmen om verbanden te leggen en patronen op te sporen kan onbedoeld tot onheuse bejegening, discriminatie, uitsluiting of stigmatisering leiden. De in de AVG genoemde profieltransparantie en uitleg van de logica van de besluitvorming is nog onvoldoende uitgekristalliseerd om voldoende houvast aan organisaties te kunnen bieden. Zorg en voorzorg ten aanzien van deze kwesties is cruciaal om het vertrouwen van betrokkenen in de dienstverlening te houden.

8.3 Maatregelen

Het uitvoeren van een ethische impact assessment, waarin de ethische consequenties van de handelingen in kaart worden gebracht, is een maatregel die organisaties kunnen treffen. Dit kan aangevuld worden met klantenpanels om deze implicaties inzichtelijk te maken en na te gaan tot welke acties dit zou moeten leiden. Speciale aandacht zouden dan de genoemde negatieve gevolgen moeten hebben: in hoeverre kan er sprake zijn van onheuse bejegening, van discriminatie, van stigmatisering, van uitsluiting? Is sprake van het gebruik van gevoelige gegevens die tot extra aandacht nopen?



Kader 5: Wetenschappelijk, historisch en statistisch onderzoek

Het verwerken van persoonsgegevens ten behoeve van wetenschappelijk, historisch en statistisch onderzoek kent enkele uitzonderingsgronden. De achtergrond hiervan is de veronderstelling dat dit onderzoek geen impact heeft op de privacy van de betrokkenen. Daar waar dat evident wel het geval is zal deze uitzonderingsgrond dan ook niet van toepassing zijn. Dit geldt bijvoorbeeld voor medisch onderzoek waar sprake is van gevoelige gegevens (die herleidbaar zijn tot individuen) en voor onderzoek waar strafrechtelijke gegevens voor gebruikt worden. De uitzonderingsgrond houdt in dat er voor wetenschappelijk, historisch en statistisch onderzoek niet opnieuw een legitieme grondslag voor de gegevensverwerking hoeft te worden gegeven. Het doel –onderzoek ten behoeve van het algemene nut – impliceert dat dit doel niet onverenigbaar is met het oorspronkelijke doel van de gegevensverzameling. Daarnaast vervalt de verplichting om betrokkenen op de hoogte te stellen van het feit dat diens gegevens voor dit doel gebruikt worden. De betrokkene kan dan ook geen rechten laten gelden op inzage, correctie en verwijdering.

9 Costs and benefits

9.1 Achtergrond

Veel organisaties beschouwen privacy als een ‘dissatisfier’, als een kenmerk waar je alleen maar negatief op kunt scoren en dat geen waarde toevoegt aan de organisatie. Zo wordt privacy ook eerder als een hindernis voor verdere innovatie beschouwd dan dat het innovaties uitlokt. Dit zijn echter achterhaalde opvattingen. Ten eerste beoordelen individuen organisaties mede op de manier waarop deze met hun gegevens omgaan. Het feit dat privacy tot nu toe nauwelijks gezien wordt als een onderwerp dat positief kan bijdragen aan de organisatiedoelen wil niet zeggen dat dat niet kan, en dat klanten en burgers dit niet zouden verwelkomen. Daarnaast brengt een goede aanpak van de omgang met persoonsgegevens evidente voordelen voor een organisatie met zich mee, zoals een efficiëntere inrichting van de gegevensprocessen, een duidelijker beeld op rollen en verantwoordelijkheden, een beperkter risico op onheus, onvoorzien of onwettig gebruik, en een positieve uitstraling naar klanten en burgers. Een goed uitgevoerde kosten-baten analyse kan helpen om voor- en nadelen beter naast elkaar te plaatsen en daarmee betere besluiten over te plegen privacy-investeringen te maken.

9.2 Uitwerking

Kosten en baten zullen naast elkaar moeten worden geplaatst. Dat is geen triviale oefening. Kosten kunnen materieel van aard zijn terwijl de opbrengsten immaterieel zijn. Kosten moeten onmiddellijk worden gemaakt terwijl baten pas na verloop van tijd worden geïncasseerd. En kosten kunnen door de ene partij moeten worden gemaakt terwijl een andere partij er de vruchten van plukt. Kosten voor het aanstellen van een data protection officer, voor het inrichten van een veilige gegevensopslag, voor het invoeren van een strikt toegangs- en authenticatiesysteem kunnen vaak wel worden vastgesteld. Moeilijker is het om de opbrengsten te benoemen: zou de organisatie op de vingers zijn getikt, zou er een datalek hebben kunnen plaatsvinden, zouden betrokkenen de organisatie gedaagd kunnen hebben omdat ze hun rechten niet konden uitoefenen? En wat is de winst van een efficiëntere organisatie, van een heldere verdeling van rollen en verantwoordelijkheden, van toegenomen vertrouwen van klanten in de organisatie?

9.3 Maatregelen

Er zijn verschillende soorten maatregelen die het uitvoeren van een kosten-batenanalyse ondersteunen. We presenteren er twee: het uitvoeren van een kosten-batenanalyse, en het opstellen van een businessmodel.

Kosten-batenanalyse

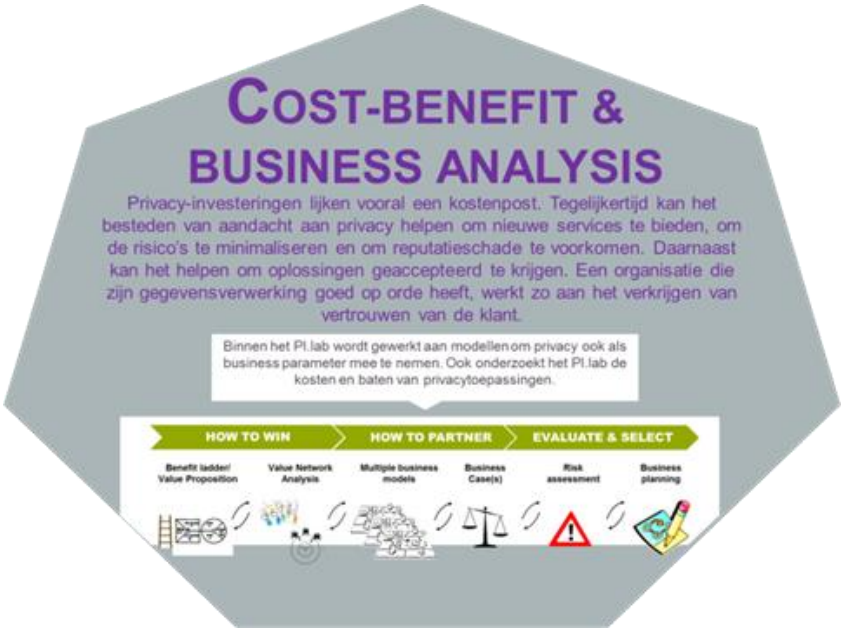
Een CBA (cost-benefit analysis) bestaat gebruikelijk uit drie, steeds complexer wordende stappen:

1. Het identificeren en vergelijken van scenario’s. Een scenario omvat keuzes betreffende de technologische architectuur, het governance model en/of de implementatie strategie. Het opstellen van een scenario geeft al veel inzicht.

2. Het kwalificeren van kosten en baten. Voor ieder scenario worden kosten en baten aangegeven en gedetailleerd. Dit kan door gebruik te maken van studie (vergelijkbare cases), workshops of expertbevraging.
3. Het kwantificeren van kosten en baten. Voor ieder scenario worden de investeringen en operationele kosten bepaald. Ook hier kan aan de batenkant gebruik worden gemaakt van bevraging van klanten via workshops, en bevraging van experts, naast formeel kwantitatieve methoden.

Business modelling
De business propositie of de dienst die een individu krijgt aangeboden kan het resultaat zijn van een samenwerking van verschillende partijen. Bij deze samenwerking kan sprake zijn van het delen en verrijken van gegevens. Dan wordt het van belang om het gehele waardeweb rond een dienst in kaart te brengen en na te gaan welke bijdrage iedere actor aan de te realiseren waarde levert. De variëteit aan rollen en na te streven waarde kan op zijn beurt weer leiden tot verschillende businessmodellen. Deze modellen kunnen dan – tot slot – beoordeeld worden op de privacyimpact voor de klant/burger en de mogelijkheden om deze impact te minimaliseren.

Het uitvoeren van zowel een kosten-batenanalyse als het opstellen van business modellen kan hand in hand gaan, en levert in gezamenlijkheid ook de beste inzichten op.



10 Transparant

10.1 Achtergrond

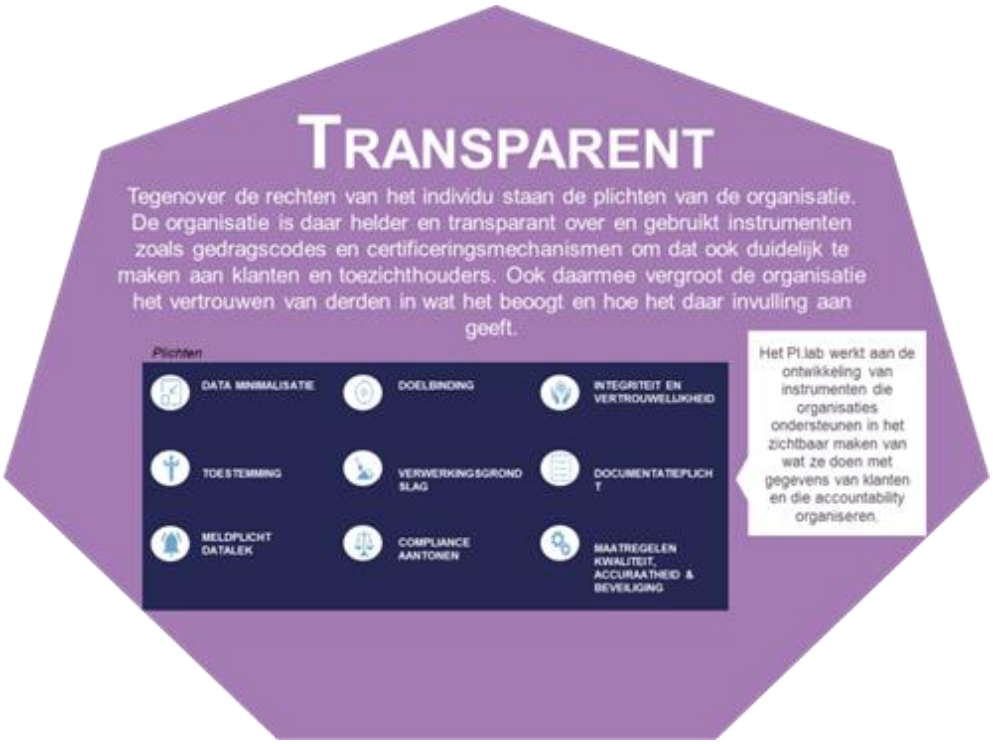
Terwijl individuen steeds transparanter in hun doen en laten worden, wordt het voor individuen steeds moeilijker om te overzien wie er wat met hun gegevens doet. Het herstellen van dit evenwicht kan ertoe bijdragen dat individuen minder wantrouwen komen te staan tegenover het delen van hun gegevens. In verschillende andere sectoren van economische bedrijvigheid is transparantie vanzelfsprekend en ook geborgd. Dit geldt voor de voedselindustrie en voor grote delen van de maakindustrie. Ook de gegevensverwerkende industrie zal dit pad op dienen te gaan, zo is onze overtuiging. Dit vraagt om het optuigen van een toegesneden systeem van transparantie dat enerzijds betrokkenen informeert over hoe een organisatie zijn gegevensprocessen heeft georganiseerd (en voor welk doel) maar anderzijds voorkomt dat mogelijke concurrentievoordelen teniet worden gedaan.

10.2 Uitwerking

De AVG legt organisaties verschillende plichten op rond de verwerking van gegevens. Op verzoek moeten organisaties inzage kunnen geven over doelen van de gegevensverwerking, betrokken derde partijen, de logica achter de gegevensverwerking en welke gegevens de organisatie over een specifiek individu bijhoudt. Ook moet een organisatie alle processen waarin sprake is van de verwerking van persoonsgegevens in kaart brengen om deze desgevraagd aan de bevoegde autoriteit te kunnen overleggen. Het uitvoeren van een DPIA en het instellen van een DPO zijn in bepaalde omstandigheden eveneens verplicht uit te voeren maatregelen. Het actief voldoen aan deze verplichtingen door helderheid te verschaffen over gegevensverwerking, doeleinden, etc. en door duidelijk te maken hoe rollen en verantwoordelijkheden binnen de organisatie zijn verdeeld, draagt bij aan het creëren van interne bewustwording voor het belang van een verantwoorde omgang met persoonsgegevens en aan een beeld naar buiten toe van een organisatie die deze verantwoording serieus neemt.

10.3 Maatregelen

De verantwoorde omgang met persoonsgegevens is niet alleen een zaak van een eventueel aan te stellen DPO. Maatregelen om transparantie in die omgang te bevorderen strekken zich uit tot alle lagen van de organisatie. Het in kaart brengen van alle processen waarbij persoonsgegevens worden verwerkt kan gepaard gaan met het toebedelen van rollen en verantwoordelijkheden. Het privacydashboard (zie Empowerment) kan verder uitgerust worden met informatie over doelen en grondslagen van gegevensverwerking, samenwerking met derde partijen, het algemene privacybeleid, verantwoordelijken binnen de organisatie, etc., etc. Daar hoort ook transparantie over DPIAs en eventuele datalekken bij.



Kader 6: Verwerkingsverantwoordelijke en verwerker

De partij die doel en middelen bepaalt van een verwerking van persoonsgegevens wordt door de AVG aangewezen als de verwerkingsverantwoordelijke (‘controller’). Deze partij is primair aansprakelijk voor het naleven van de wet met betrekking tot wat is toegestaan en wat niet. De verwerkingsverantwoordelijke kan een partij inschakelen voor de daadwerkelijke verwerking. Dat is dan de verwerker (‘processor’). Ook de verwerker heeft een zelfstandige verantwoordelijkheid voor de veilige verwerking van de gegevens en kan zich niet verschuilen achter wat de verwerkingsverantwoordelijke hem opdraagt. De afspraken tussen de verwerkingsverantwoordelijke en de verwerker worden vastgelegd in een overeenkomst. Meerdere partijen kunnen gezamenlijk de verantwoordelijkheid voor de verwerking van persoonsgegevens hebben. Ze zijn dan gezamenlijk verantwoordelijk (‘joint controllers’).

11 Vervolgstappen

In de voorgaande hoofdstukken hebben we een grote verscheidenheid aan maatregelen benoemd die een organisatie ondersteunen in de verantwoorde omgang met persoonsgegevens. De basis voor deze maatregelen wordt gevormd door de Algemene Verordening Gegevensbescherming die 25 mei 2018 formeel van kracht wordt. De AVG geeft rechten aan de betrokkenen en draagt de verwerkingsverantwoordelijken en verwerkers (zorg-)plichten op. Het schrijft niet in detail voor wat er moet gebeuren. Er is veel regelruimte en organisaties hebben de kans om zelf op gepaste wijze invulling aan hun verplichtingen te geven. Verschillende maatregelen die nu nog behoorlijk open zijn – zoals het gebruiken van *data protection by default* en *by design* – zullen in de komende jaren nader ingevuld worden. De Europese Data Protection Board – de opvolger van de huidige Artikel 29 Werkgroep – zal hier een belangrijke rol in spelen.

Technische middelen zoals op attributen gebaseerde certificaatsystemen, nieuwe encryptietechnieken en identiteits- en toegangssystemen zijn al beschikbaar en worden in lopende onderzoekstrajecten verder ontwikkeld en marktrijp gemaakt. De verplichting om *by default* en *by design* rekening te houden met privacy betekent dat het niet meer voldoende is om achteraf maatregelen te treffen. Dat moet vanaf het eerste begin in het systeemontwerp worden meegenomen.

Organisatorische maatregelen zijn eveneens noodzakelijk en dragen ook – meer dan technische maatregelen – bij aan het creëren van een verantwoorde houding binnen alle lagen van een organisatie ten aanzien van de omgang met persoonsgegevens, van klanten, van burgers. Ook hier zijn inmiddels verschillende instrumenten voor beschikbaar, die eveneens in de komende jaren verder zullen uitkristalliseren. De *data protection impact assessment* brengt risico's in kaart en stelt mitigerende maatregelen voor. Het is een instrument dat voor bredere bewustwording ten aanzien van de privacyrisico's kan zorgen, ook waar het gaat om lastiger vragen die met het gebruik van geavanceerde AI en machine learning methoden te maken hebben.

Het is nu de tijd om met de invoering van deze maatregelen te beginnen. Dat is niet alleen de verantwoordelijkheid van de organisaties die direct met de verwerking van persoonsgegevens te maken hebben. Ook brancheorganisaties, toezichthouders en andere publieke organen spelen een rol in het organiseren en verspreiden van *best practices* en geschikte instrumenten.

Het uiteindelijk doel is om te voldoen aan de wettelijk gestelde verplichtingen op een zodanige wijze dat privacy voor de organisatie gaat werken, om daarmee ook maatschappelijke behoeften te vervullen.

12 Het PI.lab

Het PI.lab is een samenwerking tussen de Radboud Universiteit (onderzoeksafdeling Digital security), Tilburg University (Tilburg Institute for Law, Technology and Society) en TNO (Roadmap Networked Information). De drie kennisinstellingen hebben hun krachten gebundeld in het onderzoek naar digitale privacy en elektronische identiteiten om zodoende bij te dragen aan de oplossing van maatschappelijke vraagstukken op dit terrein. De drie instellingen brengen zo'n 50 wetenschappers bij elkaar die zich in hun onderzoek op alle aspecten van digitale privacy en elektronische identiteiten richten: technische, juridische, organisatorische, maatschappelijke en beleidsmatige invalshoeken worden kritisch gevolgd en verder gebracht. De resultaten van het onderzoek leidt tot praktische oplossingen voor klanten.

Het PI.lab beschouwt een respectvolle aanpak van privacy als een waarde die door data gedreven innovaties weet te verbinden aan de fundamentele rechten die individuen is toegekend. Daardoor ontstaan diensten en toepassingen die voor iedereen waardevol en toegankelijk zijn. Het PI.lab onderzoekt de huidige ontwikkelingen, reflecteert hierop en bouwt op basis van die reflectie aan toegesneden oplossingen. Die oplossingen betreffen zowel de techniek als de implementatie in een maatschappelijke praktijk als de beleidsmatige sturing die voor een succesvolle implementatie gewenst is. Het doet dit door fundamenteel en toepassingsgericht onderzoek aan wet- en regelgeving, nieuwe encryptietechnologieën, methoden en technieken voor privacy by design, nieuwe businessmodellen en hulpmiddelen voor het bevorderen van transparantie van organisaties en empowerment van individuen.

Disclaimer:
Dit rapport zal gebruikt worden om te komen tot een door TNO uit te brengen white paper. Gelieve deze versie aan te halen als:
Marc van Lieshout, Somayeh Djafari, Petra Vermeulen (2017). *RESPECT4U*. TNO-rapport R10680. Den Haag: TNO/PI.lab.