DE ALGEMENE VERORDENING GEGEVENSBESCHERMING EN DE GEVOLGEN VOOR ORGANISATIES

Voor een duurzame digitale samenleving

Jan Matto

5 Februari 2018

MAZARS

INHOUDSOPGAVE

1. INLEIDING

Dit whitepaper geeft een overzicht van de belangrijkste gevolgen van de invoering van de nieuwe Algemene Verordening Gegevensbescherming (AVG) voor organisaties en de maatregelen die zoal getroffen moeten of kunnen worden om aan de AVG te voldoen.

De AVG is door het Europees Parlement aangenomen op 6 april 2016 en heeft directe werking in de lidstaten van de Europese Unie. De lidstaten moeten uiterlijk 25 mei 2018 de verordening hebben ingevoerd. Onderwerpen uit de AVG zijn in dit whitepaper geordend op basis van de privacyprincipes zoals gedefinieerd door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). Vervolgens zijn de belangrijkste uitgangpunten van de AVG per privacyprincipe becommentarieerd en zijn aanwijzingen gegeven voor te treffen maatregelen. Hierbij is ook breed gebruik gemaakt van overige literatuur en richtsnoeren uitgegeven door onder meer de Autoriteit Persoonsgegevens (AP). Dit whitepaper heeft niet tot doel om volledig te zijn of om alle mogelijke risico's en maatregelen te inventariseren. Dit paper geeft achtergrondinformatie en een handreiking hoe het brede en complexe vraagstuk van privacy- en gegevensbescherming op een gestructureerde en verantwoorde wijze kan worden benaderd.

1.1. Achtergronden bij privacy- en gegevensbeveiliging

Onze samenleving en economie zijn de afgelopen decennia sterk gedigitaliseerd. Deze ontwikkeling zet zich nog steeds exponentieel voort. De digitalisering geeft ongekende mogelijkheden voor mens, maatschappij en bedrijven en overheden. De digitalisering kent naast positieve kanten ook keerzijden. Keerzijden zijn onder meer:

- Inbreuken op de grondbeginselen van de rechten van de mens
- Identiteitsfraude
- Datalekken
- Cybercrime
- Digitale economische delicten
- Verstoringen van vrije marktwerking
- Ontstaan van monopolistische infrastructuren en internetdiensten
- Ontstaan van vitale en kwetsbare infrastructuren en verstoringen daarvan
- Nieuwe bedrijfs-, bestuurlijke en politieke risico's
- Cyberoorlog en cyberspionage

Wet- en regelgeving lopen achter op deze ontwikkelingen als gevolg van de steeds verdergaande digitalisering en een veranderend gebruik. Denk hierbij aan ontwikkelingen als The Internet of Things en inzet van Big Data. De overheid is echter bezig met een inhaalslag.

De komende tijd zullen regelmatig nieuwe wetten en regels worden ingevoerd en aangescherpt om de digitalisering in goede banen te leiden. Autoriteiten krijgen grotere bevoegdheden en sanctioneringsmogelijkheden. Het verantwoord omgaan met digitale systemen en gegevensverzamelingen staat op gelijke voet met andere duurzaamheidsaspecten, zoals mensenrechten, klimaat en milieu. Steeds meer organisaties beginnen in te zien dat het beschermen van de privacy van individuen opgenomen in digitale gegevensverzamelingen belangrijk is. Het netjes omgaan met persoonsgegevens zegt iets over het respect van een organisatie voor haar cliënten, veelal ook de cliënten van haar cliënten en de samenleving als geheel. Meer en meer wordt het aantoonbaar compliant zijn met privacywet- en regelgeving en het in dat verband beveiligen van persoonsgegevens een randvoorwaarde om mee te mogen doen in de digitale economie. Privacybescherming en gegevensbeveiliging zijn aansluitvoorwaarden. De consument, markt en maatschappij willen zekerheid en transparantie over hoe persoonsgegevens worden verwerkt en beschermd. Uiteindelijk is het doel het realiseren van een duurzame digitale samenleving en economie.

1.2. Privacy is een grondrecht en digitalisering een inbreuk daarop

Gebruik van persoonsgegevens, zowel in de private als in de publieke sector, vormt in veel gevallen een inperking van het grondrecht van bescherming van de persoonlijke levenssfeer.[1] Uit dit gebruik ontstaan risico's voor de persoonlijke levenssfeer (privacy) van de betrokkenen. Onzorgvuldigheid, onbetrouwbaarheid van gegevens, verlies van gegevens, de controle over gegevens (datalekken) en het gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen, kunnen een ernstige negatieve impact hebben op iemands sociaal en maatschappelijk welbevinden.

Vanuit het Europese Verdrag van de Rechten van de Mens (EVRM) is dan ook aangegeven dat elke digitale vastlegging van persoonsgegevens een inbreuk is op de rechten van de mens. De verantwoordelijke voor deze digitale vastlegging dient passende maatregelen te treffen om de inbreuk te beperken. Door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) zijn al in de jaren '80 van de vorige eeuw definities gemaakt van de privacyprincipes die nageleefd moeten worden om de rechten van de mens te kunnen eerbiedigen. Het gaat in dit verband om de informationele privacy van het individu. In 2013 is hiervan een geactualiseerde versie verschenen.[2] Deze privacyprincipes zijn de basis voor de bestaande wetgeving, de Wet Bescherming Persoonsgegevens (WBP), de meldplicht datalekken en een reeks van sectorale wetten. Ook binnen de aankomende AVG zijn deze principes nog steeds de basis. De bestaande en nieuwe privacywetgeving geeft de kaders aan waarbinnen persoonsgegevens verwerkt mogen worden en de maatregelen voor het beschermen van deze gegevens én de privacy van betrokkenen. [3] De AVG richt zich dus ook op de informationele privacy.

De regelgeving loopt flink achter op wat inmiddels in de digitale samenleving en economie plaatsvindt. De voortschrijdende technologische ontwikkeling impliceert ook dat de regelgeving voorlopig dynamisch zal blijven. Een continue stroom van nieuwe regels en voorschriften is daarvan het gevolg, waarop organisaties en gegevensverwerkende systemen moeten worden aangepast. Belangrijke bronnen om te volgen voor nieuwe kaders en richtlijnen zijn publicaties van de AP, de Working Party 29 van de Europese Commissie en instituten zoals nationale en internationale overheidsorganisaties voor cybersecurity. In Nederland is dat het Nationaal Cyber Security Centrum. Voorts geeft de Nederlandse Orde van Register EDP Auditors (NOREA) diverse richtlijnen en handreikingen uit voor Privacy Audits en Privacy Impact Assessments.

Informatietechnologie en grootschalige digitale gegevensverwerkingen kunnen additionele (privacy)risico's introduceren die inherent zijn aan de inzet van deze technologie, maar die niet direct zichtbaar zijn op het niveau van het eindgebruik; denk aan de risico's van metadata. Metadata zijn door systemen gegenereerde persoonsgegevens over digitaal gedrag als gevolg van het gebruik van deze systemen. Het gebruik van internettechnologie impliceert nu eenmaal dat in de technische middelen informatie ontstaat over IP-adressen, websitebezoek, zoekgedrag, wie met wie in contact staat, de locatie waar iemand zich bevindt, et cetera. Met deze gegevens kunnen persoonlijke voorkeuren en situaties worden afgeleid en kunnen profielen worden gemaakt. Inmiddels kunnen ook apparaten gekoppeld aan het internet veel informatie onthullen over individuen. Denk aan smartphones webcamera's, thermostaten, slimme meters, garagedeuren, verlichting, et cetera. Al deze apparaten (The Internet of Things) generen persoonsgegevens die kunnen worden gebruikt voor profiling en introduceren privacyrisico's. De AVG wijst uitdrukkelijk op de risico's hiervan en schrijft dwingend technische maatregelen voor om deze risico's te bestrijden.[4] Generatie en gebruik van metadata is veelal niet transparant voor de betrokkenen en is daarmee een inbreuk op de regelgeving. Inmiddels worden meer persoonsgegevens gegenereerd door

[1] Zie artikel 10, lid 2 en 3 Grondwet, artikel 8 EVRM en artikel 8 EU-Grondrechtenhandvest.

[2] Zie de OESO publicatie: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

[3] De op 13 december 2017 gepubliceerde concept uitvoeringswet AVG toont dat deze inhoudelijk dicht bij de Europese AVG blijft en ook dichtbij de bestaande Wbp vereisten blijft.

[4] De AVG wijst uitdrukkelijk op de risico's van het koppelen van natuurlijke personen aan online identificatoren via apparatuur, applicaties, IP-adressen, cookies, RFID-technologie, et cetera (pag. 17, overweging 30).

het gebruik van systemen en apparaten dan persoonsgegevens die rechtstreeks worden ingevoerd in systemen.

Naast privacyrisico's brengt de digitalisering van onze samenleving en economie ook andere risico's met zich mee die hieraan gerelateerd zijn en een relatie hebben met de te treffen privacybeschermingsmaatregelen in organisaties en systemen. Dit betreft risico's als gevolg van het ontstaan van vitale digitale infrastructuren met potentiële gevolgen voor bedrijfsvoering en samenleving. Het ongelimiteerd verzamelen en/of lekken van persoonsgegevens geeft verstoringen van vrije mededinging en marktwerking. De effecten hiervan worden momenteel door de Nederlandse overheid onderzocht. Onrechtmatige verwerkingen als gevolg van het niet naleven van de privacywet- en regelgeving worden in lijn hiermee meer en meer gezien als economische delicten.

1.3. Highlights uit de Algemene Verordening Gegevensbescherming

Op 6 april 2016 heeft het Europees Parlement de Algemene Verordening Gegevensbescherming aangenomen. Deze verordening heeft directe werking in de lidstaten van de Europese Unie. De lidstaten hebben tot 25 mei 2018 de tijd om de verordening in te voeren.

Versterking rechten van betrokkenen
In de nieuwe verordening zijn de rechten van betrokkenen aanzienlijk versterkt. Organisaties moeten de rechten van betrokkenen eerbiedigen en de betrokkenen de mogelijkheid geven om hun rechten uit te kunnen oefenen. Zo moet er onder meer toestemming worden gevraagd aan de betrokkenen voor het verwerken van gegevens, moet de verwerking transparant zijn en hebben betrokkenen recht op inzage, correctie en 'vergetelheid' van hun gegevens. Bovendien moet voor elke verwerking van persoonsgegevens worden vastgesteld of deze rechtmatig is, een gerechtvaardigd belang dient, proportioneel is gegeven het doel en of de doelstellingen van de verwerking niet op een andere wijze met minder persoonsgegevens kunnen worden gerealiseerd (subsidiariteit).

Dataminimalisatie en specifieke doelstellingen
Uitgangspunt is dat bij de verwerking van persoonsgegevens de data wordt geminimaliseerd en dat het gebruik alleen binnen vastgelegde doelstellingen plaatsvindt. Gegevens worden alleen bewaard binnen het kader van een specifiek doel, gegevens worden niet langer bewaard dan strikt noodzakelijk en gegevens worden niet onnodig verspreid.

Verantwoordelijkheid
Voor elke verwerking van persoonsgegevens moet een verwerkingsverantwoordelijke partij zijn aangewezen. De verwerkingsverantwoordelijke dient te zorgen dat de verwerking voldoet aan de eisen die voortvloeien uit de verordening. Indien de verwerking is uitbesteed aan een externe partij, een verwerker, dan blijft de verwerkingsverantwoordelijke verantwoordelijk voor de naleving van de eisen die voortvloeien uit de verordening. De verwerker moet dan aan de verwerkingsverantwoordelijke kunnen aantonen dat de benodigde maatregelen effectief zijn.

Periodieke toetsing
Compliant zijn aan de privacywet- en regelgeving vereist dat periodiek wordt geïnventariseerd welke privacyrisico's zich voordoen en welke maatregelen daartegenover staan. Daarbij moet worden vastgesteld of de gebruikte persoonsgegevens daadwerkelijk noodzakelijk zijn voor de te bereiken doelstellingen. Hierbij speelt zowel de vraag naar proportionaliteit (is de specifieke gegevensverwerking nodig om het doel te bereiken?) als de subsidiariteit (zijn er geen minder privacy-bedreigende alternatieven of waarborgen mogelijk). Een middel hiervoor is een Privacy Impact Assessment (PIA). Een PIA is sinds 2013 verplicht binnen de Nederlandse overheid. Vanaf 25 mei 2018 geldt deze verplichting ook voor de private sector, afhankelijk van de omvang van de organisatie en de omvang en gevoeligheid van de verwerking.

Permanente bescherming en periodieke audits
Verder stelt de verordening dat verwerkingen van persoonsgegevens beveiligd moeten zijn. Hiervoor dient de verwerkingsverantwoordelijke dan wel de verwerker, passende organisatorische én technische beveiligingsmaatregelen te treffen. Hierbij wordt de kanttekening geplaatst dat de beveiligingsmaatregelen moeten zijn ingericht 'naar de stand van de techniek'. Bovendien dienen de verwerkingsverantwoordelijke en een eventuele verwerker over het vermogen te beschikken om permanent de bescherming van persoonsgegevens te garanderen en daar periodieke controles op uit te voeren. Belangrijk daarbij is om te onderkennen dat het de integriteit, vertrouwelijkheid, authenticiteit en beschikbaarheid van gegevens betreft. Oftewel, gegevens moeten niet alleen veilig en vertrouwelijk worden verwerkt, maar moeten ook kloppen en geraadpleegd kunnen worden.

Technische beveiligingsmaatregelen zijn de basis
De AVG geeft aanwijzingen tot het verplicht treffen van technische maatregelen als het gaat om het verwerken van persoonsgegevens. Ter vermijding van profiling op basis van digitale identifiers wordt bijvoorbeeld effectieve pseudonimisering als privacy bevorderende maatregel voorgeschreven. Het bijhouden van registers en logfiles voor het detecteren en analyseren en zondig het monitoren van de beveiligingssituatie zijn randvoorwaardelijke maatregelen. De verwerkingsverantwoordelijke moet de toegang tot persoonsgegevens op basis van need-to-know te hebben ingericht. Voorzieningen moeten zijn getroffen om dit waar te kunnen maken.

Organisatorische maatregelen
Organisaties vanaf een bepaalde omvang kunnen door de AVG worden verplicht om een functionaris aan te stellen voor gegevensbescherming. Deze functionaris heeft bevoegdheden om onafhankelijk onderzoek te doen naar de bescherming van persoonsgegevens en naleving van wet- en regelgeving. De functionaris voor de gegevensbescherming verzorgt ook eventuele contacten met de AP.

Forse sancties
Tot slot krijgen de autoriteiten aanzienlijk meer sanctioneringsmogelijkheden om naleving van de verordening te handhaven. Dit kan in de vorm van het opleggen van hoge boetes die voldoende afschrikkend zijn. Dat wil zeggen dat boetes kunnen oplopen tot een maximum van 4% van de wereldwijde jaaromzet van een organisatie van €20 miljoen. Zelfs het verbieden van verwerkingen van persoonsgegevens behoort tot de mogelijke sanctioneringen.

Voor wie geldt de AVG?
De AVG geldt voor alle organisaties, groot, klein en ook voor bijvoorbeeld ZZP'ers die persoonsgegevens verwerken. Voor sommige maatregelen zoals het aanstellen van een Functionaris voor de Gegevensbeschermingen gelden drempels en criteria voor deze verplichting. De criteria zijn gebaseerd op de omvang van de verwerkingen van persoonsgegevens en de gevoeligheid daarvan. Voor het inrichten van het register van verwerkingen geldt een verplichting vanaf 250 medewerkers of als sprake is van een "niet-incidentele" verwerking. In de praktijk betekent dit volgens de informatie van de Autoriteit Persoonsgegevens zelf dat dit register vrijwel altijd een verplichting is. Verwerkingen hebben zelden een incidenteel karakter.

2. ANALYSE VAN DE AVG OP BASIS VAN UNIVERSELE PRIVACYPRINCIPES EN –RISICO'S

2.1. Toelichting

De universele privacyprincipes en -risico's zijn de basis voor de huidige wet- en regelgeving en zijn ook de basis geweest voor de Algemene Verordening Gegevensbescherming, die op 6 april 2016 in het Europees Parlement is vastgesteld. Deze verordening heeft directe werking in alle EU-lidstaten. Alle lidstaten moeten deze verordening uiterlijk op 25 mei 2018 hebben ingevoerd.

De privacyprincipes en -risico's geven het perspectief van waaruit de toezichthoudende autoriteiten en het maatschappelijk verkeer op een organisatie en haar gegevensverwerkingen zullen kijken. Een organisatie moet per principe kunnen uitleggen hoe naleving is gerealiseerd. Voor de privacyrisico's moet een organisatie per risico kunnen aantonen welke maatregelen zijn getroffen om het risico in te perken.

Belangrijk is dat onderkend wordt dat het gaat om wat een organisatie daadwerkelijk doet met persoonsgegevens. Deze gedigitaliseerde werkelijkheid (de IT-werkelijkheid) wordt bepaald door de technische architectuur, gebruikte technologieën en inrichting van systemen. Zonder inzicht in deze IT-werkelijkheid is het niet mogelijk om de vragen over de compliance aan privacyprincipes en/of vragen over de beheersing van risico's voldoende te beantwoorden. Bij ieder vraagstuk omtrent informationele privacybescherming dient in elk geval inzicht te bestaan in de verwerking van data in alle technische systeemlagen. Dus ook de risico's van metadata dient te worden begrepen.

In de volgende hoofdstukken zijn privacyprincipes ontleend aan de algemene OESO-privacyprincipes. Deze principes zijn aangevuld met inzichten uit het model Privacy Impact Assessment Rijksoverheid en de handreiking voor het uitvoeren van een Privacy Impact Assessment van de NOREA.

Privacyprincipes en privacyrisico's vertonen onderlinge relaties en afhankelijkheden. Principes en risico's kunnen elkaar versterken, maar ook verzwakken. Per situatie moet de wijze waarop de principes en risico's zich aandienen worden geëvalueerd en moet worden vastgesteld of maatregelen toereikend zijn. De context is hierin een allesbepalende factor.

Per privacyprincipe worden bij benadering de volgende risico's onderkend:

PRIVACYPRINCIPE	Privacyrisico's								
	ID	DD	FC	IV	NT	NE	DL	OB	GC
1. Verantwoording		x	x	x	x	x	x		
2. Limiteren van het verzamelen van gegevens	x	x	x				x		x
3. Doelbinding / limiteren van het gebruik van gegevens	x	x	x		x	x	x		x
4. Gegevenskwaliteit	x							x	
5. Beveiliging van gegevens (Privacy by Design/ Privacy Enhancing Technologies)	x	x	x			x		x	
6. Transparantie					x	x	x	x	
7. Rechten van betrokkenen					x	x	x	x	x

- ID: Identiteitsfraude
  - DD: 'Data deluge'-effect
- WA: Waardestijging van persoonsgegevens
- FC: Function creep
  - OU: Onrechtmatig gebruik van uniek identificerende gegevens
  - PF: Profiling
  - VB: Verkeerde behandeling in sociaal en economisch maatschappelijk verkeer
  - SK: Stigmatisering door koppeling van gegevens
- IV: Inconsistente implementatie en naleving verantwoordingsbeginsel
- NT: Geheime (niet transparante) verwerking van persoonsgegevens
- NE: Niet toegestane verwerking van persoonsgegevens buiten de EU
  - CC: Nieuwe ontwikkelingen op het terrein van cloud computing waarbij gegevens over de hele wereld kunnen worden verplaatst.
- DL: Datalekken, waaronder onrechtmatige toegang, verlies van data, cybercrime, ontstaan van ongewenste risicovolle metadata
- OB: Omkering van de bewijslast voor de betrokkene
- GC: burgers worden gedwongen om in te stemmen met het gebruik van hun gegevens

Bovenstaande tabel geeft ook aan dat er een onderlinge wisselwerking is tussen zowel de privacy-principes als de privacyrisico's. Dit betekent dat het onderzoeken van privacy en gegevensbescherming al gauw veelzijdig en complex kan zijn. Bij elk privacy-onderzoek zullen beleidsmatige, functionele, technische, organisatorische en juridische aspecten een rol moeten spelen.

2.2. Universele privacyprincipes

De basis voor elk privacyvraagstuk (bijvoorbeeld een Privacy Impact Assessment of Privacy Audit) ligt in het identificeren van risico's ten aanzien van de zogenaamde privacyprincipes. De algemene privacy-principes zijn gebaseerd op de OESO definities 2013 met aanvullingen uit de WBP en de AVG. Op basis van een literatuurstudie zijn uit verschillende documenten de aanvullingen op deze principes gemaakt,

welke relevant zijn voor de inrichting of toetsing van een ontwerp of bestaand systeem voor de verwerking van persoonsgegevens.

2.2.1. Verantwoording (accountability)

Verantwoordelijken nemen maatregelen om materiële beginselen uit de AVG te vertalen naar differentieerbare programma's (nalevingsprogramma's).[5] De nalevingsprogramma's worden gebaseerd op PIA's[6] om privacyrisico's te elimineren of te mitigeren. Het geheel wordt vertaald naar concrete maatregelen en procedures op strategisch, tactisch en operationeel niveau. De borging kan aan externe belanghebbenden, met inbegrip van de AP, worden bewezen door monitoring en door interne of externe audits. De verwerkingsverantwoordelijke moet aantonen hoe invulling is gegeven aan privacyprincipes en of de privacyrisico's voldoende zijn afgedekt. Dit betekent uiteraard dat het verantwoordelijke management tevens over een verantwoordings- en rapportagesysteem moet beschikken om 'in control' te zijn op de universele privacyprincipes. Vast onderdeel is dat de verwerkingen en de onderliggende technologie en de bijbehorende risico's inzichtelijk moeten zijn. Niet transparante verwerkingen van persoonsgegevens zijn verboden.

De monitoring betreft zowel de monitoring op organisatie- en bedrijfsprocessen (gedrag van individuen) als de monitoring op de technische systemen, de handhaving van de gegevensbeveiliging, de verwerkingen, de toegang tot persoonsgegevens, de verstrekkingen van data aan derde partijen en de partijen die de rol van verwerker vervullen.

Teneinde invulling te kunnen geven aan de verantwoordelijkheid is een eerste vereiste volgens de AVG dat een register wordt bijgehouden van alle verwerkingen van persoonsgegevens.[7] Daarbij is het nodig dat persoonsgegevens op attribuutniveau en per categorie van betrokkenen bekend zijn. Het register dient tevens beschrijvingen te bevatten van de technische en organisatorische beveiligingsmaatregelen, bewaartermijnen van gegevens, hoe gegevens worden gewist en welke overige partijen bij de verwerking betrokken zijn. Dat betekent dat een verantwoordelijke en een eventuele verwerker duidelijkheid moet kunnen geven over de technische en organisatorische inrichting van verwerkingen. Dit vereist een behoorlijke kennis van het ontwerp én de daadwerkelijke werking van gebruikte informatietechnologie.

Het ontbreken van een dergelijk register impliceert direct dat niet is voldaan aan de AVG. In feite kan worden gesteld dat de betreffende organisatie geen controle heeft over de door haar uitgevoerde verwerkingen en dus ook geen invulling kan geven aan de overige privacyprincipes en bijbehorende vereisten.

Samengevat:
Verantwoording kan alleen worden gedragen als tenminste:

- Een register beschikbaar is van de verwerkingen met beschrijvingen van de persoonsgegevens (attributen)
- Doelstellingen van de verwerkingen specifiek zijn beschreven en er een gerechtvaardigd belang is (de overheid heeft een wettelijke grondslag)
- Inzicht bestaat in de aard van de verwerkingen van persoonsgegevens en de categorieën van persoonsgegevens van betrokkenen
- Een risicoanalyse beschikbaar is omtrent de gevoeligheid van de gegevens en de aard van de verwerkingen
- Documentatie beschikbaar is hoe informatiestromen lopen (gegevensverzameling, -verwerking en verstrekkingen aan derde partijen)

[5] Artikel 24 e.v. AVG: Verantwoordelijkheid van de Verwerkingsverantwoordelijke
[6] Artikel 35, AVG. De AVG spreekt van een gegevensbeschermingseffectbeoordeling in plaats van een Privacy Impact Assessment. In dit paper houden wij vast aan de terminologie Privacy Impact Assessment (PIA).
[7] Artikel 30, AVG: Register van verwerkingsactiviteiten

- Duidelijk is met welke IT-middelen de verwerking plaatsvindt (ongeacht of deze intern of extern zijn belegd)
- Een overzicht beschikbaar is van de getroffen technische en organisatorische beveiligings-maatregelen
- De verantwoordelijkheden voor de verwerkingen van persoonsgegevens duidelijk zijn belegd, bijvoorbeeld middels een informatiebeveiligingsbeleid en –plan
- De nalevingsprogramma's worden gebaseerd op PIA's om privacyrisico's te elimineren of mitigeren
- Het geheel is vertaald naar concrete maatregelen en procedures op strategisch, tactisch en operationeel niveau
- De borging aan externe belanghebbenden, met inbegrip van de AP, kan worden bewezen door monitoring van de beveiliging en interne of externe audits
- Ook de overige privacyprincipes aantoonbaar voldoende zijn ingevuld.

Let op: deze opsomming van vereisten is niet limitatief, maar betreft kernpunten uit de AVG.

Elke organisatie moet per verwerking vaststellen of zij de verwerkingsverantwoordelijke dan wel verwerker is. Indien de verwerking is uitbesteed aan een verwerker moet een schriftelijke overeenkomst worden opgesteld met instructies voor de verwerker aangaande de beveiliging en behandeling van de persoonsgegevens.[8] Daarbij dient de verwerker middels inspecties of audits op verzoek van de verwerkingsverantwoordelijke aan te tonen dat de instructies van de verwerkingsverantwoordelijke worden nageleefd. Dit is tevens een vereiste in de AVG, ook wel de right-to-audit genoemd. [9]

Een waarschuwing is hier op zijn plaats. De verwerkingsverantwoordelijke dient aantoonbaar én controleerbaar haar beveiligingsbeleid op te leggen aan een verwerker. Voor verwerkers is dat lastig omdat niet alle verwerkingsverantwoordelijken een gelijk beveiligingsbeleid hebben. De vraagstelling wie verwerkingsverantwoordelijke of verwerker is, moet per casus te worden bekeken. Andere sectorale wet- en regelgeving, zoals de Telecomwet en de Wet Geneeskundige Behandelovereenkomst (WGBO), kan een belangrijke rol spelen bij de vaststelling van de verhoudingen tussen verwerkingsverantwoordelijke en verwerker. Niet in alle gevallen is evident welke partij verwerkersverantwoordelijke is en welke partij verwerker is. Het kan voorkomen dat partijen karakteristieken van beide hebben. In dat geval kan het nodig zijn om verwerkingen te splitsen en inrichtingen van systemen hierop aan te passen, om op die manier toch zuivere verhoudingen te creëren.

Voor de verwerker geldt onder meer dat deze een register moet bijhouden van de verwerkingsactiviteiten die ten behoeve van de verwerkingsverantwoordelijke worden uitgevoerd.[10] Daarbij behoort ook het verstrekken van inzicht in de getroffen technische en organisatorische beveiligingsmaatregelen.

Het kortste artikel van de AVG, artikel 31, beschrijft dat de verwerkingsverantwoordelijke en de verwerker in voorkomende gevallen mee moeten werken met de AP bij de vervulling van haar taken. Hiermee wordt bedoeld dat de AP desgevraagd inzage moet kunnen krijgen in de getroffen maatregelen en aard van verwerkingen. Voorbereiding hierop is uiteraard belangrijk.

2.2.2. Transparantie

Individuen, consumenten en burgers moeten te worden geïnformeerd over het gebruik van hun persoonsgegevens in samenhang met de gebruikte technologie en dienen daarover controle uit te kunnen uitoefenen. Het individu (de betrokkene) is hierdoor in staat om bepaalde vormen van verwerking of onrechtmatig gedrag in rechte aan te vechten.

[8] Artikel 28, lid 3 e.v., AVG
[9] Artikel 28, lid 3, sub h, AVG
[10] Artikel 30, lid 1 e.v., AVG

Transparantie impliceert dat een volledig gedocumenteerd inzicht nodig is in de architectuur en inrichting van de verwerkingen, ook als de verwerkingen zijn uitbesteed aan een verwerker. Daarnaast moet duidelijk en controleerbaar zijn welke functionarissen toegang hebben tot welke systemen. In elk geval moet worden voorkomen dat er ontransparantie ontstaat over de verwerkingen of het gebruik van gegevens. Dit kan alleen indien de volledige datastroom en alle daarvoor gebruikte middelen bekend zijn en de aard van het gebruik van gegevens door functionarissen duidelijk is.

Casus
Een verwerkingsverantwoordelijke maakt gebruik van een App-ontwikkelplatform dat via de cloud ter beschikking wordt gesteld. Nadere analyse van deze tool toont aan dat 'onderwater' persoonsgegevens, waaronder IP-adressen, van betrokkenen voor analysedoeleinden worden verstuurd naar de bouwers van het App-ontwikkelplatform. Dit was bij de verwerkingsverantwoordelijke niet bekend en is dus ook nooit medegedeeld aan de betrokkenen op het moment dat zij toestemming gaven voor het verwerken van persoonsgegevens. Dit is een overtreding van de AVG.

Dergelijke niet transparante verwerkingen kunnen middels een combinatie van penetratietesten, codereviews en het monitoren of meten van uitgaand berichtenverkeer middels tooling worden onderkend. Periodieke toetsingen en rapportages over de bevindingen zijn belangrijk om dergelijke niet transparante systeemwijzigingen te vermijden. Bij grote en complexe verwerkingen van persoonsgegevens en systeemomgevingen is de inzet van tooling nagenoeg onvermijdelijk.

2.2.3. Doelbinding

Persoonsgegevens worden alleen voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en niet verder verwerkt als dat onverenigbaar is met de doeleinden. Dit is een ontwerpprincipe voor een inzichtelijk functionerende informatieinfrastructuur, zowel functioneel, beveiligingstechnisch als organisatorisch.

Ook om aan de verantwoordings- en transparantieprincipes invulling te kunnen geven is het essentieel en vereist conform de huidige WBP en de AVG dat van elke verwerking van persoonsgegevens een specifieke en beperkte doelstelling is vastgelegd. Deze doelbinding is, naast dat het een verplichting betreft, belangrijk om informatiearchitecturen te kunnen ontwerpen die aan de AVG voldoen en een randvoorwaarde om aan betrokkenen duidelijk te maken met welk beperkt doel de persoonsgegevens worden verwerkt. Een beperking in het doel geeft tevens aanwijzingen voor een beperking in het gebruik hetgeen ook een verplichting is vanuit de AVG. De doelbinding is daarnaast relevant om een betrokkene, op het moment dat toestemming moet worden gevraagd voor verwerking van persoonsgegevens, te infomeren over het doel van de verwerking en het daarbij passende gebruik van persoonsgegevens.

De doelbinding vereist een aantal formele vastleggingen die gekoppeld zijn aan het eerder genoemde register van gegevensverwerkingen. Het bewaken van de doelbinding vereist periodieke toetsing van de inrichting van systemen, de beveiliging van gegevens en systemen, alsmede de verrichte verstrekkingen van gegevens. Zowel van de interne verstrekkingen van gegevens binnen de organisatie als verstrekkingen aan derde partijen dient beoordeeld te worden of deze passend zijn gegeven de doelbinding. Systeemwijzigingen vormen een duidelijke bedreiging voor het doelbindingsprincipe. Het periodiek toetsen van systeemwijzigingen op niet toegestane 'function creep' is belangrijk om het doelbindingsprincipe te handhaven.

Indien persoonsgegevens worden verstrekt aan derde partijen blijft de verwerkingsverantwoordelijke verantwoordelijk voor de handhaving van de doelbinding. Ook na verstrekking dient er sprake te zijn van een vooraf gespecificeerde beperkte doelstelling voor het gebruik. Dit impliceert dus maatregelen voor de beveiliging van de gegevens, limitering van de toegang tot gegevens voor alleen daartoe bevoegde functionarissen en limitering van het gebruik voor een specifiek beschreven doel bij de ontvangende derde partij.

Casus
Het UWV levert gegevensdiensten aan derde partijen. Hiertoe heeft het UWV een zogenaamde UWV-audit opgezet. Afnemers van de UWV-gegevensdiensten dienen periodiek een audit uit te laten voeren naar de opzet, werking en het bestaan van maatregelen voor bescherming van persoonsgegevens. Onderdeel van deze audit is een toetsing van gerealiseerde beveiliging en toegangscontrole tot de verstrekte gegevens op basis van het 'need-to-know' en 'need-to-have' principe. De auditor toetst het gebruik van de gegevens aan vooraf vastgestelde doelstellingen zoals vastgelegd in een overeenkomst met het UWV. Dit is een voorbeeld hoe een organisatie de doelbinding kan bewaken, ook in het geval van verstrekkingen aan derde partijen.

2.2.4. Noodzakelijkheid en limitering van verzamelen en gebruik van persoonsgegevens (gegevensminimalisering)

De inrichting van een informatiesysteem dient op het ondersteunen van het specifieke doel te zijn toegespitst. Identificatie en traceerbaarheid van het individu mogen niet langer duren dan strikt noodzakelijk is. Minimalistisch gegevensgebruik, ofwel datalimitering en limitering van het gebruik, is het uitgangspunt. Concreet betekent dit dat de gegevens enkel toegankelijk mogen zijn voor functionarissen die de gegevens nodig hebben voor hun functie.

Limitering van het verzamelen en het gebruik van persoonsgegevens kan op een aantal gebieden plaatsvinden. Allereerst dienen de vragen te worden gesteld of het doel van de verwerking niet op een andere, minder privacy-belastende wijze kan worden gerealiseerd met minder data en of de verwerking van de persoonsgegevens daadwerkelijk noodzakelijk is. Dit is een vraagstuk dat in een ontwerpfase thuishoort en onderdeel is van 'Privacy-by-Design'. Privacy-by-Design is een aanpak die de AVG eveneens hanteert en ook binnen een PIA dient te worden gedresseerd.[11]

Een ander belangrijk ontwerpcriterium om te voldoen aan het principe van limitering van het verzamelen en het gebruik van persoonsgegevens is het treffen van maatregelen die de toegang tot gegevens beperken. Dit kan door het realiseren van een logische toegangsbeveiliging waardoor enkel functionarissen toegang hebben tot de gegevens die noodzakelijk zijn voor het uitvoeren van hun taak op een wijze die passend is binnen de geformuleerde doelbinding. Dit vereist het hanteren van toegangsbeveiliging op basis van 'need-to-know' en 'need-to-have'.[12] Technische voorzieningen en een juiste inrichting daarvan zijn noodzakelijk om hieraan te kunnen voldoen. Controleerbaarheid van de logische toegangsbeveiliging wordt zonder een juiste inrichting van de techniek omslachtig. Het niet hanteren van deze uitgangspunten voor de toegang tot persoonsgegevens kan al gauw leiden tot een niet-proportionele toegang tot gegevens en dient als datalek te worden beschouwd. Vooral bij de verwerking van gevoelige persoonsgegevens dient de toegang en het gebruik beperkt te zijn en te worden gemonitord.

De logische toegangsbeveiliging omvat zowel de identificatie (wie ben je?), authenticatie (ben je het echt?) als de autorisatie (wat mag je?). Daarbij is controleerbaarheid een vereiste. Elke functionaris met toegangsrechten dient daarom te beschikken over een unieke gebruikerscode, zodat middels waarnemingen in het systeem is vast te stellen of de toegangsrechten daadwerkelijk juist zijn ingeregeld volgens de vastgelegde principes, eventuele afwijkingen kunnen worden gedetecteerd en zo nodig corrigerende maatregelen kunnen worden getroffen. Zowel de opzet van de toegangsbeveiliging als de werking dient toetsbaar te zijn. Dit laatste vereist ook logging faciliteiten van de toegang tot systemen en gegevens. Zie voor verdere uitwerking paragraaf 2.2.8 Beveiliging.

[11] De termen Privacy by design (PbD) en Privacy enhancing Technologies (PET) zijn niet als zodanig in de AVG genoemd, maar zijn in de 'Richtsnoeren beveiliging van persoonsgegevens' beschreven (Autoriteit Persoonsgegevens 2013).
[12] Deze termen komen niet voor in de AVG, maar zijn in de 'Richtsnoeren beveiliging van persoonsgegevens' beschreven (Autoriteit Persoonsgegevens, 2013). Een andere term hiervoor is: 'least priveleged principle'.

2.2.5. Rechtmatige grondslag

Persoonsgegevens dienen uitsluitend te worden verwerkt op basis van de limitatieve grondslagen zoals in de AVG en de huidige WBP is vastgelegd. Dit impliceert een verwerking op basis van een expliciete toestemming van betrokkenen, een overeenkomst, een wettelijke verplichting, een publieke taak of een gerechtvaardigd belang.

Het gebruik van persoonsgebonden nummers, zoals het BSN, wordt bij wet geregeld. Bij verwerkingen van dergelijke gevoelige persoonsgegevens of indien er sprake is van omvangrijke verwerkingen kan, op basis van een uitgevoerde risicoanalyse en/of een PIA en voorafgaand aan de realisatie van de verwerking, de AP om advies worden gevraagd. Voor het gebruik van BSN geldt specifieke wetgeving.

Dit onderwerp vereist naast het BSN-domein ook in andere sectoren aandacht. Het kan voorkomen dat een afweging moet worden gemaakt tussen de privacybescherming van betrokkenen en bijvoorbeeld een gewichtig maatschappelijk belang dat een verwerking rechtmatig maakt, ondanks de inbreuk op de individuele privacy. Deze afwegingen moeten van geval tot geval worden bepaald.

Er bestaat een scala aan sectorale wetten en regels die afhankelijk van de situatie een rol kunnen spelen bij het vaststellen van een rechtmatige grondslag. Het voert voor dit paper te ver om dat hier nader uit te werken.

2.2.6. Kwaliteit

Voorafgaand aan de start van een verwerking dient in een procedure te worden vastgelegd aan welke kwaliteitseisen die verwerking en de daarmee gemoeide persoonsgegevens moeten voldoen. Kwaliteitseisen worden zoveel mogelijk via de functionaliteit van een informatiesysteem afgedwongen. De AVG stelt dat de integriteit van persoonsgegevens permanent moet worden gegarandeerd, door het treffen van technische en controlemaatregelen. Denk hierbij naast het beveiligen tegen ongeautoriseerde toegang en onrechtmatige mutatie van gegevens ook aan controlemaatregelen waarbij persoons-gegevens gevalideerd worden of data analyses worden uitgevoerd, mogelijk zelfs profilingtechnieken en patroonherkenning, waarmee afwijkingen kunnen worden gedetecteerd. Deze controlemaatregelen lijken op gespannen voet te staan met het handhaven van vertrouwelijkheid. Toch kan voor de verwerkingsverantwoordelijke een gerechtvaardigd belang bestaan om deze controles in te voeren. Zorgvuldigheid en transparantie blijven uiteraard belangrijk.

Casus

In het geval van het verwerken van gevoelige persoonsgegevens, zoals digitale identiteitsgegevens (digitale identifiers), dient een afweging te worden gemaakt tussen het belang van vertrouwelijkheid van de verwerking van deze persoonsgegevens en het belang om eventuele identiteitsfraude te detecteren. Immers, de AVG stelt niet alleen de eis dat persoonsgegevens beveiligd moeten zijn vanuit het oogpunt van vertrouwelijkheid, maar ook dat de integriteit geborgd moet zijn. Het beschermen van de integriteit van digitale identiteiten is belangrijk ter vermijding van identiteitsfraude. Hiertoe zijn, mede gezien de eis van de permanente garantie van de bescherming van persoonsgegevens, controlemaatregelen vereist die het karakter hebben van profiling, patroonherkenning en detectie van ongebruikelijke identificaties en transacties. Deze maatregelen impliceren een inbreuk op de privacy van betrokkenen. Het standpunt kan echter worden ingenomen dat deze inbreuken niet opwegen tegen een groter maatschappelijk belang, namelijk het bestrijden van identiteitsfraude en het voorkomen van schade die door andere betrokkenen kan worden geleden. Dit is een belangrijk aandachtpunt in bijvoorbeeld de Privacy Impact Assessment uitgevoerd op het ontwerp van het nieuwe Nederlandse Identiteiten stelsel (eID-Stelsel) en de Privacy Impact Assessment op de opvolger van DigiD, DigiD Substantieel.[13][14]

[13] Privacy Impact Assessment eID Stelsel 1.0, www.idensys.nl, Mazars, 2015

[14] Privacy Impact Assessment DigiD Substantieel 1.0, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/10/02/aanbieding-privacyrapportage-digid-substantieel, Mazars, oktober 2017

2.2.7. Bewaren

Persoonsgebonden gegevens worden niet langer bewaard dan voor een specifiek doel noodzakelijk is. De AVG stelt dat persoonsgegevens moeten worden vernietigd zodra dat mogelijk is. Over het algemeen zijn specifieke maatregelen nodig om aan deze eis tegemoet te kunnen komen. Het kan nodig zijn om in een database ontwerpvelden op te nemen met markeringen voor het geautomatiseerd of gedifferentieerd vernietigen van gegevens. Een organisatie dient aannemelijk te kunnen maken dat gegevens kunnen worden gewist en dat deze in specifieke situaties ook werkelijk zijn gewist.

Indien gegevens worden verwerkt van kwetsbare groepen dan kan het volgens de AVG noodzakelijk zijn om niet alleen de persoonsgegevens van kwetsbare groepen extra te beveiligen, maar ook om deze gegevens bijvoorbeeld met prioriteit te wissen. Een kwetsbare groep is bijvoorbeeld minderjarigen. Het kan nodig zijn om in een ontwerp op voorhand met deze functionele eisen rekening te houden (Privacy by Design) en Privacy Enhancing Technologies toe te passen. Bijvoorbeeld door gegevens direct bij vastlegging te oormerken met een kenmerk op basis waarvan na een vastgestelde periode de gegevens automatisch worden gewist.

2.2.8. Beveiliging

Passende technische en organisatorische beveiligingsmaatregelen dienen te worden genomen tegen verlies of enige vorm van onrechtmatige verwerking op basis van een risico-analyse. Dat kunnen zowel preventieve als detectieve of repressieve maatregelen zijn. Daarbij wordt rekening gehouden met de stand van de techniek en de kosten van de implementatie (uitvoeringskosten). Onnodige verzameling en verdere verwerking van persoonsgegevens moet worden voorkomen. Een periodieke rapportage over de gerealiseerde beveiligingsmaatregelen en de effectieve werking daarvan maken onderdeel uit van deze eis. Organisaties dienen volgens de eisen van de AVG over het vermogen te beschikken om de veiligheid van gegevens permanent te garanderen en periodiek nalevingsprogramma's uit te voeren.

Organisatorische maatregelen richten zich op het realiseren en implementeren van een informatiebeveiligingsbeleid en een informatiebeveiligingsplan. Het informatiebeveiligingsplan dient te voorzien in voldoende handvaten voor de medewerkers over de manier waarop zij om dienen te gaan met de verwerking van persoonsgegevens. Uiteindelijk dienen begrijpelijke, werkbare en controleerbare procedures te zijn ingericht.

Het periodiek evalueren van de werking van de organisatorische maatregelen dient een onderdeel te zijn van het totale beveiligingsplan. Hierbij verdient het aanbeveling om acties te ondernemen rond beveiligingsbewustzijn door bijvoorbeeld tests uit te voeren, waarbij door aangewezen functionarissen wordt vastgesteld of onrechtmatige toegang tot persoonsgegevens mogelijk is. Denk hierbij aan vooropgezette phising campaigns, security audits en penetratietesten.

Informatiebeveiliging vereist vooral ook technische maatregelen. Vaak wordt gesteld dat de mens de zwakste schakel is en daarmee de techniek minder belangrijk is. Dit wekt helaas een verkeerde indruk. Immers, een slecht beveiligd gedigitaliseerd systeem kan niet worden gecompenseerd door een mens. Dat kan worden vergeleken met het besturen van een auto zonder remmen, veiligheidsriemen en achterlichten door een automobilist met een goede rijinstructie. De auto moet veilig zijn. Dit geldt hetzelfde voor een geautomatiseerde verwerking van persoonsgegevens.

De AVG stelt dan ook zeer duidelijk dat persoonsgegevens moeten worden beveiligd naar de stand van de techniek en dat daarbij een kostenafweging moet worden gemaakt. Hier geldt wederom het

proportionaliteitsprincipe. Naarmate de gevoeligheid en het volume van gegevens toenemen zijn meer stringente beveiligingsmaatregelen vereist.[15]

De AVG geeft eveneens aan dat het treffen van beveiligingsmaatregelen met het oog op netwerk- en informatiebeveiliging, het monitoren van die informatiebeveiliging en het handhaven van een bepaald vertrouwelijkheidsniveau verantwoordelijkheden zijn van de verwerkingsverantwoordelijke. Doel daarbij is bescherming tegen onrechtmatige toegang, kwaadaardige acties en incidentele gebeurtenissen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de verzamelde gegevens in het gedrang brengen en beveiliging van de hiermee verband houdende diensten die door netwerken of systemen worden geboden. Denk bij dat laatste aan beveiligingsmaatregelen tegen virussen, malware, denial of service en anderssoortige aanvallen op computers en netwerken. Middelen die hiervoor kunnen worden ingezet zijn firewalls, intrusion detection en/of prevention systemen, antimalware software. Zogenaamde remote wipe services kunnen worden toegepast om gegevens op gedistribueerde systemen en remote devices te kunnen wissen indien deze in mogelijk verkeerde handen zijn gevallen.

Het treffen van dit soort beveiligingsmaatregelen tegen ongeautoriseerde toegang en andere incidenten impliceert dat medewerkers en betrokkenen actief in systemen worden gemonitord en dat securityloggings worden aangelegd om inbreuken en ongeautoriseerde toegang te kunnen vaststellen. Hoewel dit een inbreuk tot gevolg kan hebben op de privacy van individuen kan sprake zijn van een gerechtvaardigd belang om deze instrumenten in te zetten en dergelijke verzamelingen van persoonsgegevens aan te leggen. Hier geldt overigens dat de privacyprincipes onverkort van toepassing blijven. De risico's van dergelijke verwerkingen van persoonsgegevens dienen juist te worden ingeschat en de beveiliging van beveiligingslogbestanden zelf dient aan hoge eisen te voldoen. De praktijk leert dat dergelijke monitoring en het aanleggen van securitylogs in zekere zin ook weer securityrisico's introduceren. Zorgvuldigheid blijft hierbij zeer belangrijk. Het afschermen van beveiligingsmaatregelen en logbestanden tegen misbruik en manipulatie is essentieel. Een systemadministrator mag logfiles niet kunnen wijzigen of weggooien. Handhaving van functiescheidingen binnen de IT-organistatie en -systemen is een belangrijke maatregel (Segregation of Duties).

De AVG vermeldt dat zij technologieneutraal is. Daarmee wordt bereikt dat er geen marktbeïnvloeding plaatsvindt, een level playing field wordt gehandhaafd voor leveranciers van beveilgingsmiddelen en ook de houdbaarheid van de AVG wordt hiermee vergroot. Immers, de digitale technologie is nog steeds in ontwikkeling. Wat vandaag veilig is, kan morgen achterhaald zijn. De AVG stelt simpelweg dat de beveiliging naar de stand van de technologie moet zijn opgezet en dat daarbij een kosten-/batenafweging moet worden gemaakt. Toch biedt de AVG, zij het zeer beperkt, wel enige aanwijzingen.

Zo worden pseudonimisering en versleuteling van persoonsgegevens als maatregelen verplicht gesteld waar dit als passend wordt geacht om de privacybescherming van betrokkenen te verhogen.[16] Daarbij wordt tevens de aanwijzing gegeven dat het beheer van sleutels of andere attributen die een pseudo-identiteit of geanonimiseerde gegevens kunnen herleiden, in een andere omgeving dienen te worden bewaard en alleen toegankelijk mogen zijn voor daartoe gemachtigde functionarissen. Beveiliging van deze sleutels en attributen is essentieel alsook een passende 'sleutelprocedure'.

Een andere belangrijke verplichting die is opgenomen in de AVG is 'het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en -diensten te garanderen'. Dit betreft ook het vermogen om fysieke of technische incidenten als het gaat om de beschikbaarheid van de toegang tot persoonsgegevens te herstellen.

Het bovenstaande impliceert, vanwege de eis van permanente garantie door de verwerkings-verantwoordelijke dat maatregelen worden getroffen die het mogelijk maken dat de beveiliging én de

[15] AVG, Pag. 160, Artikel 32 ev
[16] AVG, Pag. 160, Artikel 32, lid 1 a

kwaliteit van persoonsgegevens periodiek worden getoetst, danwel dat er voorzieningen zijn getroffen die de beveiliging en kwaliteit van de persoonsgegevens monitoren. Het implementeren van mechanismen en technische voorzieningen om afwijkingen en inbreuken realtime te signaleren kunnen hierbij zowel effectief als efficiënt zijn. Hier geldt wederom dat een risicoafweging en een afweging van uitvoeringskosten moet worden gemaakt. Voor het afleggen van verantwoording of voor het uitvoeren van privacy en security audits is essentieel dat voldoende bewijsvoering uit de technische systemen zelf kan worden verkregen.

Privacy Enhancing Technologies (PET)
Deze term wordt niet als zodanig in de AVG genoemd. Echter in het document: 'Richtsnoeren Bescherming Persoonsgegevens', van de Autoriteit Persoonsgegevens wordt op de noodzaak van toepassing van PET gewezen. In de AVG wordt benoemd dat bijvoorbeeld pseudonimisering en het versleutelen van gegevens als technieken moeten worden toegepast om de privacy te beschermen. Met pseudonimisering wordt de herleidbaarheid van identificerende sleutels naar een individu bemoeilijkt en de risico's op profiling teruggedrongen. De toepassing van PET is daarnaast opgenomen in de eis dat gegevensbescherming naar de stand van de techniek moet worden gerealiseerd. PET omvat een samenhangend systeem van ICT-maatregelen, dat de privacy beschermt door het elimineren, verminderen of voorkomen van onnodige en/of ongewenste verwerking van persoonsgegevens, zonder dat hierbij de functionaliteit van een informatiesysteem wordt aangetast. De Nederlandse overheid heeft aangegeven het voortouw te nemen bij de inzet van PET.

De AVG wijst specifiek op de inzet van pseudonimisering om de risico's van grootschalig gebruik van digitale identifiers te vermijden. Denk hierbij aan de binnen de internettechnologie bestaande mogelijkheden om betrokkenen te profileren door gebruik van IT-dienstaanbieders die een rol spelen in tussenliggende communicatieschakels. Het gebruik van sectorale, tijdelijke non-persistente pseudoniemen en polymorfe pseudoniemen worden in de literatuur als mogelijke maatregelen gezien om de risico's op profiling te beperken. Pseudoniemen worden echter door de AVG nog steeds, terecht, als persoonsgegevens beschouwd. De reden is dat aan de hand van sleutels of door het koppelen van gegevens het nog steeds mogelijk is om van een pseudoniem de werkelijke identiteit van de betrokkene te achterhalen. Pseudonimisering kan echter wel de privacybescherming van betrokkenen verhogen, bijvoorbeeld doordat intermediaire partijen en IT-dienstverleners in de informatieketen waarbinnen gegevens worden uitgewisseld, de werkelijke identiteiten achter de pseudoniemen moeilijker kunnen herleiden. De verwerkingsverantwoordelijke moet de gegevens die de mogelijkheid geven om de pseudoniemen te herleiden afzonderlijk bewaren en borgen dat alleen gemachtigde personen toegang hebben tot deze gegevens. Dergelijke gegevens, die in feite een sleutel bieden tot identiteiten, vereisen uiteraard een sterke beveiliging. De AVG geeft echter ook aan dat het gebruik van pseudoniemen niet bedoeld is om andere gegevensbeschermingsmaatregelen uit te sluiten.[17] PET kent een veelheid van vormen en implementaties en is nog sterk in ontwikkeling. Pseudonimisering is slechts één van de mogelijke maatregelen.

Voor onderzoeksdoeleinden en data-analyse wordt aanbevolen om persoonsgegevens te anonimiseren en zo mogelijk deze alleen te gebruiken op een hoger aggregatieniveau zodat herleiding naar individuen niet mogelijk is.

Privacy by Design (PbD)
Gegevensbescherming inclusief PET zijn van meet af aan een onderdeel van het ontwerp van de architectuur van het informatiesysteem. ECP/EPN beveelt PbD in de brede maatschappelijke context van het ontwikkelen van digitale diensten of producten aan als privacybeschermende maatregel. De beginselen van **noodzakelijkheid, proportionaliteit en subsidiariteit** worden hierin meegenomen. Deze verplichting geldt vanaf de design- tot en met de beheerfase van ICT-projecten. De infrastructuur van een informatiesysteem dient op de bestaande mogelijkheden en inzichten van PbD en PET te worden gereviseerd en in lijn te worden gebracht met de actuele stand van de technieken die die principes mogelijk

[17] AVG, Pagina 16, overweging 28

verdergaand hanteert. Dit kan op basis van afwegingen betekenen dat het implementeren van PET eerst bij de noodzakelijke vervanging van (componenten in) een ICT-infrastructuur of bij een volgende generatie informatiesystemen in de vorm van PbD aan de orde komt.
Privacy by Design wordt niet in deze termen gebruikt in de AVG. Echter in de verplichting om per verwerking een PIA uit te voeren en daarbij, voordat de verwerking in gebruik is genomen, de maatregelen en mechanismen vast te stellen, zodat aan alle vereisten van de verordening is voldaan, is Privacy by Design de facto een verplichting geworden.[18]

Casus
In de visie van de AP is een infrastructurele aanpak onontbeerlijk om fundamentele waarden als privacy op lange termijn te garanderen. Er ontwikkelt zich een maatschappij brede digitale identiteitsinfrastructuur voor de overheid en bedrijfsleven, die de basis zal vormen voor haar informatie-infrastructuur. Pseudo-identiteiten zijn volgens de AP een onmisbaar gereedschap bij privacybescherming in informatiesystemen. Niet-kenbaarheid van het individu is daarom een essentieel ontwerpprincipe voor de identiteitsinfrastructuur van de overheid. Persoonsgebonden nummers spelen een belangrijke rol bij identiteitsmanagement. Nummerstelsels blijken moeilijk te beheren en te beheersen. Vanuit informatiekundig perspectief valt er daarom veel te zeggen voor een gedifferentieerde aanpak waarin verschillende keten- en sectornummers naast elkaar bestaan en een overkoepelende identifier wordt vermeden. In de huidige praktijk betekent dit dat veel bestaande systemen in architectuurontwerp herziening behoeven. Met deze inzichten is het BSN in Nederland een zeer privacy-onvriendelijk nummerstelsel vanwege de grote sector overschrijdende profiling risico's.

2.2.9. Rechten van betrokkenen
Individuen hebben naast het recht op transparantie, het recht op inzage, correctie, aanvulling, afscherming of verwijdering van hun persoonsgegevens en het recht zich tegen de verwerking ervan te verzetten. Een individu mag periodiek opvragen aan welke instanties zijn persoonsgegevens zijn verstrekt en hiervan een overzicht ontvangen. De functionaliteit van ICT-infrastructuur dient op het effectueren van deze rechten te zijn toegerust.

Deze eisen vanuit de AVG impliceren dat een verwerkingsverantwoordelijke in staat moet zijn om aan de rechten van betrokkenen te voldoen. Dit vereist maatregelen in een organisatie en in de functionaliteit van de technische systemen, zoals het bijhouden van een register van alle verstrekkingen aan derde partijen en inzicht in de bestanden waarin de gegevens van individuen zijn opgenomen. Dit is bijvoorbeeld essentieel om de betreffende gegevens te kunnen wissen. Bij het ontwerp van systemen is hier specifiek aandacht voor nodig.

Daarnaast kan men overwegen om specifieke tooling in te zetten om te monitoren waar gegevens van individuen naar toe worden verspreid. Het versnipperen van persoonsgegevens door onzorgvuldig databeheer maakt het moeilijk om garantie te kunnen geven voor voldoende beveiliging en maakt het zeker ook moeilijk om deze gegevens gegarandeerd te kunnen wissen.

Niet over het hoofd mag worden gezien, en de AVG is daar ook duidelijk over, dat indien een rechthebbende een verzoek tot inzage doet en inzicht verlangt van wat er met zijn of haar persoonsgegevens gebeurt, de verwerkingsverantwoordelijke zich eerst zekerheid verschaft over de identiteit van de aanvrager, zodat voorkomen wordt dat persoonsgegevens worden verstrekt aan niet-rechthebbenden. Omgekeerd dient de verwerkingsverantwoordelijke bij het vastleggen van persoonsgegevens ook haar identiteit aan de betrokkene te onthullen alvorens om toestemming voor vastlegging van persoonsgegevens wordt gevraagd. Het is voor de hand liggend, maar de praktijk leert dat dit vaak niet correct wordt uitgevoerd.

[18] AVG, Pag. 166, Artikel 35, lid 7

3. ALGEMENE PRIVACY RISICO'S

3.1. Inleiding

Het verwerken van persoonsgegevens kan risico's voor de privacy van het individu opleveren. Risico's staan meestal niet op zichzelf; ze zijn soms in elkaar verweven, kunnen elkaar sterk beïnvloeden en laten zich daarom niet scherp afbakenen. De onderstaande algemene of universele risico's die zich in de maatschappij kunnen voordoen, zijn ontleend aan literatuuronderzoek. Voortdurende actualisering van deze ontwikkelingen aangaande privacy en data protection risico's is essentieel.

3.2. 'Data deluge'-effect

Het 'data deluge'-effect houdt in dat de hoeveelheid persoonsgegevens die beschikbaar is, wordt verwerkt en wordt doorgegeven, blijft groeien. Dit fenomeen wordt versterkt door zowel technologische ontwikkelingen, dat wil zeggen de groei van informatie- en communicatiesystemen, als door het feit dat individuen steeds beter in staat zijn gebruik te maken van en te reageren op technologieën. Naarmate er meer gegevens beschikbaar zijn en mondiaal worden uitgewisseld, neemt ook het risico voor de privacy toe. Denk hierbij aan het ontstaan van metadata, big data en data analytics.

De AVG is in brede zin en in haar totaliteit bedoeld om dit nadelige effect voor privacybescherming aan te pakken. Het 'data deluge'-effect kan alleen worden bestreden door de vastlegging van persoonsgegevens te beperken, PET toe te passen en een sterke beveiliging van systemen en gegevens te handhaven. Maatregelen zoals extra bescherming van digitale identifiers en in het bijzonder online identifiers, inzet van pseudo-identiteiten, versleuteling en permanente waarborging van de gegevensbeveiliging zijn duidelijke voorbeelden van maatregelen ter beperking van het 'data deluge'-effect. Anonimisering en het gebruik van data aggregation zijn middelen om het gebruik van persoonsgegevens te beperken. Bijvoorbeeld bij het uitvoeren van data-analyse en big data toepassingen.

Het 'data deluge'-effect is een paraplubegrip voor de risico's die hierna aan de orde komen.

3.3. Waardestijging van persoonsgegevens

Almaar toenemende hoeveelheden persoonlijke informatie gaat gepaard met een waardestijging in sociaal, politiek en economisch opzicht. In bepaalde sectoren, met name in onlineomgevingen, zijn persoonsgegevens *de facto* een betaalmiddel geworden voor toegang tot onlinecontent. Recent onderzoek wijst uit dat bedrijven de neiging hebben om omvangrijke verzamelingen persoonsgegevens aan te leggen zonder specifiek doel. Die ontwikkeling wordt mogelijk gemaakt door de snelle daling in de kosten voor digitale opslag en wordt gedreven door het besef dat persoonsgegevens een economische hulpbron zijn die moet worden geëxploiteerd. Adverteerders en fraudeurs zorgen voor een bloeiende markt voor persoonsgegevens.[19] Waardestijging is een prikkel voor cybercrime en economisch misbruik.

De AVG stelt uitdrukkelijk dat ongelimiteerd gebruik van persoonsgegevens zonder een specifiek doel en zonder toepassing van het transparantiebeginsel niet is toegestaan. De AVG gaat zelfs zover dat, indien persoonsgegevens worden gebruikt voor direct marketing doeleinden, de betrokkene daar altijd bezwaar tegen kan maken. Ook als de verwerkingsverantwoordelijke deze persoonsgegevens van een derde partij heeft verkregen.

[19] Bron: Study on the economic benefits of privacy-enhancing technologies (PETs), Final report to The European Commission DG Justice, Freedom and Security, prepared by London Economics, July 2010, p.65.

3.4. Function creep

Function creep is het risico van het verschuiven van de doeleinden waarvoor de persoonsgegevens aanvankelijk mochten worden gebruikt. Dit risico kan ontstaan bij steeds groter groeiende databases met persoonsgegevens. In de loop van de tijd kan het inzicht of de behoefte ontstaan om die gegevens voor heel andere doeleinden te gaan gebruiken, dan ooit bij de aanleg van de database de bedoeling was.[20]

Het periodiek uitvoeren van een PIA kan helpen om de function creep te beteugelen.

3.5. Onrechtmatig gebruik van uniek identificerende gegevens

Het van overheidswege uitgegeven BSN als uniek identificerend gegeven voor een persoon zorgt voor ongekende mogelijkheden, om in geval van een breed maatschappelijk gebruik personen te volgen en te profilen. Dit kan zich uiteraard ook voordoen in geval dat betaalrekeningnummers als uniek identificerende gegevens worden gebruikt.

Profilen kan optreden als het BSN wordt gebruikt om de effectiviteit, efficiency en betrouwbaarheid van administratieve processen te bevorderen, door hieraan allerlei andere soorten van persoonsgegevens te koppelen. Identificatie via het BSN opent voor de burger in toenemende mate de poort naar dienstverlening door de overheid en het bedrijfsleven.[21]

Hierdoor neemt ook het risico van identiteitsfraude toe.[22] In dat verband wordt ook verwezen naar het risico van geheime (niet transparante) verwerking van persoonsgegevens.

Als gevolg van deze ontwikkelingen kunnen individuen langdurig en intensief onderhevig zijn aan onterechte en ongewenste bejegening in het sociaal en maatschappelijk verkeer.[23] Die gevolgen zijn nauwelijks onomkeerbaar of herstelbaar. Dit geldt ook voor uniek identificerende gegevens zoals biometrische gegevens en persistente pseudo-identiteiten die tot individuele personen herleid kunnen worden.[24] Het is nauwelijks mogelijk om, in het geval dat de BSN van iemand is gecompromitteerd, een nieuwe BSN te verkrijgen. Voor biometrische persoonsgegevens, zoals bijvoorbeeld verkregen uit lichaamsmonsters of DNA, geldt eveneens dat extra beveiligingsmaatregelen benodigd zijn. Zo is een gedigitaliseerde DNA-string per definitie niet te anonimiseren. Bronherleiding is mogelijk als een ander DNA-sample beschikbaar en gekoppeld is aan een individu. Voor DNA geldt bovendien dat de privacy van toekomstige generaties in het geding kan komen. Dit kan al het geval zijn met bepaalde medische gegevens of zeldzame ziektebeelden welke bijna identificerend kunnen zijn. Een zelfde gevoeligheid geldt ook voor digitale vastleggingen van irisscans, handpalm en vingerafdrukken. Naarmate dergelijke uniek identificeerbare gegevens meer in het maatschappelijk verkeer worden verspreid, neemt het risico van het gebruik ervan buiten de wettelijk gestelde grenzen toe.

3.6. Inconsistente implementatie en naleving verantwoordingsbeginsel

Vanwege de veelheid van partijen die bij de verwerking van persoonsgegevens (verantwoordelijken en verwerkers) zijn betrokken, varieert het niveau van privacybescherming bij de betrokken verantwoordelijkheden en verwerkers. Vooral door het ontstaan van zogenaamde informatieketens neemt dit vraagstuk toe. Hierdoor ontstaan zwakke schakels in de keten van de verwerkingen van persoonsgegevens. Zwakke schakels kunnen een cumulatief effect veroorzaken waardoor het niveau van

[20] Zie de meningen over dit risico in Happy Landings, het Biometrisch Paspoort als Zwarte Doos, Vincent Böhre, verkennende studie voor het rapport i-Overheid, WRR, oktober 2010.
[21] Het BSN mag alleen worden gebruikt als daarvoor een wettelijke basis aanwezig is.
[22] De vrees voor dit risico wordt bevestigd door de verkennende studie van CenTERdata en ECP-EPN in opdracht van de Wetenschappelijk Raad voor het Regeringsbeleid ECP-over rolverdeling van de overheid en de burger bij het beschermen van de identiteit, november 2010. Zie als bron ook noot 37.
[23] Dit risico geldt vanzelfsprekend ook voor het achterlaten van digitale sporen door de burgers zelf in de social networks.
[24] Zie ook Elektronische overheid en privacy, Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid, College bescherming persoonsgegevens, A&V 25, p. 17.

de bescherming van persoonsgegevens in een neerwaartse spiraal terecht komt. Hierdoor kan de bescherming van de persoonlijke levenssfeer op onderdelen worden aangetast. Het kan ook zijn, dat door de inconsistentie of incorrecte toepassing van de privacyprincipes door een partij in de keten, de verwerking van persoonsgegevens wordt belemmerd bij die partij. Dit leidt niet alleen tot privacyrisico's, maar ook tot onnodige bureaucratie en additionele kosten.[25] Convergentie van privacy maatregelen binnen een informatieketen is een belangrijk aandachtspunt om de privacybescherming transparant en efficiënt te houden.

3.7. Geheime (niet transparante) verwerking van persoonsgegevens

Indien een verwerking niet transparant is voor een betrokkene kan de verwerking onder omstandigheden zonder zijn toestemming, tegen zijn voorkeuren of anderszins onrechtmatig plaatsvinden. Doordat betrokkenen niet op de hoogte zijn van het gebruik van hun persoonsgegevens, kunnen zij de impact ervan in het sociaal maatschappelijk verkeer niet overzien. Zij hebben hier niet of nauwelijks controle meer over. Dit kan betekenen dat zij, zonder zich hiervan bewust te zijn, worden gestigmatiseerd en/of uitgesloten van sociaal maatschappelijke voorzieningen. In het geval dit bewustzijn ontstaat, is soms zonder buitengewone inspanningen niet te achterhalen wat de oorzaak van de nadelige effecten is. Hierdoor is de burger ook niet of nauwelijks meer in staat om zijn wettelijke privacy rechten te effectueren. Net als bij onrechtmatig gebruik van uniek identificerende gegevens, kunnen de gevolgen onomkeerbaar en onherstelbaar zijn.

3.8. Niet toegestane verwerking van persoonsgegevens buiten de EU

Doorgifte van persoonsgegevens naar landen buiten de EU en EER naar landen zonder adequaat privacybeschermingsniveau herbergt op voorhand een hoog risico van onrechtmatige verwerkingen van persoonsgegevens, alsmede het niet kunnen effectueren van rechten van betrokkenen. Persoonsgegevens worden slechts naar een land buiten de Europese Unie (EU) en de Europese Economische Ruimte (EER) doorgegeven indien dat land een passend privacybeschermingsniveau waarborgt. Dat wil zeggen dat een vergelijkbaar privacy regime bestaat met hetgeen dat in de AVG is vastgelegd.

De AVG geeft aan dat in dat geval sprake is van een concern met vestigingen buiten de EER waarmee persoonsgegevens worden uitgewisseld er bindende afspraken dienen te worden gemaakt met deze vestigingen waarbij de privacybeschermende maatregelen op het juist niveau zijn geborgd (Corporate Binding Rules). Dus dat betrokkenen ervanuit mogen gaan dat aan de vereisten van de AVG is voldaan ook als gegevens met landen worden gedeeld buiten de EER.

Recente ontwikkelingen als gevolg van de onthullingen door Snowden over PRISM en de Amerikaanse afluisterpraktijken hebben in de politiek geleid tot een herziening van afspraken die zijn gemaakt met de Amerikaanse overheid inzake het 'Safe Harbour Principe'. Dit heeft geleid tot een afsprakenstelsel onder de naam 'Privacy Shield' waarvan de houdbaarheid door deskundigen wordt betwijfeld.

3.9. Datalekken

Ten gevolge van datalekken of inbreuken in de informatiebeveiliging kunnen persoonsgegevens in handen komen van onbevoegden of kunnen verloren gaan. Persoonsgegevens kunnen verloren gaan met nadelige gevolgen voor de betrokkenen. Het verloren gaan van persoonsgegevens is in een dergelijk geval een datalek. Het uitvoeren van een onrechtmatige verwerking, bijvoorbeeld indien de toegang tot persoonsgegevens te breed is toegestaan, is ook een datalek. De meldplicht datalekken is een onderdeel van de AVG.

[25] Zie naar analogie Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions, A comprehensive approach on personal data protection in the European Union, Brussels 4.11.2010, COM(2010)609 final.

Grote databases van overheidsdiensten en private partijen zijn gevoelig voor datalekken en onbevoegde uitwisseling van persoonsgegevens.[26] Cliënten en individuen hebben in de regel geen weet van dergelijke datalekken. Hierdoor zijn zij vatbaar voor de gevolgen van alle hiervoor genoemde risico's, die afhankelijk van de aard en omvang van het datalek, progressief in omvang kunnen toenemen.

Het besluit meldplicht datalekken dat per 1 januari 2016 in Nederland van kracht is gegaan, impliceert dat, in geval van een datalek, de AP binnen 72 uur dient te worden geïnformeerd en zo nodig dienen ook alle betrokkenen die nadeel kunnen ondervinden van het datalek op de hoogte te worden gesteld. Organisaties dienen faciliteiten te hebben om aan deze verplichtingen te kunnen voldoen.

In de definitie van het AP is een datalek niet alleen het in verkeerde handen vallen van een bestand met persoonsgegevens. Het verlies van de controle over een deel van een systeem of een bestand, onrechtmatige toegang, disproportionele toegang tot data, een malware-aanval of het verloren gaan van persoonsgegevens zijn datalekken. Er zijn administratieve eisen hoe omgegaan wordt met beveiligingsincidenten, datalekken en er geldt een bewaarplicht van gegevens omtrent incidenten. Het niet voldoen aan de meldplicht datalekken kan leiden tot hoge bestuurlijke boetes oplopend tot € 820.000 of 10% van de jaaromzet van een organisatie. Deze boetes wijken dus af van de boetebevoegdheden die in de AVG staan beschreven.

Organisaties dienen beveiligingsmaatregelen te treffen om de risico's van datalekken te beperken en ook maatregelen te treffen om een datalek te kunnen vaststellen en om de juiste en tijdige acties te kunnen ondernemen. Een crisis- en communicatieplan is hier onderdeel van.

3.10. Overige privacyrisico's

Voorbeelden van overige privacyrisico's, die weer kunnen voortvloeien uit één of meer van de voorgaande risico's, zijn:

- Profiling wordt expliciet als ernstig risico genoemd in de AVG. Van personen worden profielen gemaakt op basis van bijvoorbeeld hun leefpatroon, bestedingspatroon, betaalgedrag, eetgewoonten op basis waarvan zij worden gekarakteriseerd, in maatschappelijke klassen worden ingedeeld of op een bepaalde manier in het maatschappelijk verkeer worden bejegend. [27]
- Verkeerde behandeling in het maatschappelijk verkeer als gevolg van fouten en niet transparant handelen. De AVG vereist maatregelen om de integriteit van persoonsgegevens te handhaven
- Stigmatisering door koppeling van gegevens.
- Omkering van de bewijslast voor de betrokkene omdat de betreffende gegevens nu eenmaal in een database voorkomen en door de verantwoordelijke als juist worden bestempeld. "De computer zegt dat …"
- Individuen worden gedwongen om in te stemmen met het gebruik van hun persoonsgegevens voor diverse doelen, met het oog op bijvoorbeeld het verkrijgen van diensten, gunsten of direct marketing doeleinden. [28]

[26] Bron: Study on the economic benefits of privacy-enhancing technologies (PETs), Final report to The European Commission DG Justice, Freedom and Security, prepared by London Economics, July 2010, p.67. Zie ook Happy Landings, het Biometrisch Paspoort als Zwarte Doos, Vincent Böhre, verkennende studie voor het rapport i-Overheid, WRR, oktober 2010.
[27] Deze risico's zijn het gevolg van ongewenste combinatie van niet direct tot personen te herleiden gegevens. Door het combineren van gegevens uit verschillende verwerkingen, onder andere via onderliggende technische systeemlagen of via gegenereerde loggegevens en metadata, kunnen gegevens die niet direct tot personen zijn te herleiden, alsnog tot individuen herleid worden. Ongewenste cumulatie of samenbundeling van gegevensverwerkingen, loggegevens als gevolg van gegevenstransport en andere metadata leidt tot het ondermijnen van privacyprincipes.
[28] Bron: Study on the economic benefits of privacy-enhancing technologies (PETs), Final report to The European Commission DG Justice, Freedom and Security, prepared by London Economics, July 2010, p.66-67.

- Nieuwe ontwikkelingen als 'cloud computing' waardoor de digitale ruimte voor persoonsgegevens en applicaties wordt beheerd door veel verschillende (sub)bewerkers verspreid over diverse continenten. Data wordt regelmatig verplaatst, waardoor de relevante jurisdictie veranderd. [29]
- Activiteiten van inlichtingen- en afluisterdiensten. Al dan niet geoorloofde activiteiten van interne of externe inlichtingen- en afluisterdiensten ondermijnen de veiligheid van systemen en privacy-principes. Ander aspect van dit fenomeen is dat veiligheid en transparantie wordt ondermijnd en ongewenste cumulatie en combinatie van data wordt gerealiseerd, waardoor verborgen hotspots ontstaan. Bovendien duiden recente berichten over activiteiten van inlichtingendiensten erop dat onder meer veiligheid ondermijnende malware wordt ingezet en diensten van providers worden gecompromitteerd.

Specifieke risico's ten aanzien van biometrische identificatie en authenticatie
Door de EU Working Party 193 worden ten aanzien van biometrische systemen de volgende risico's onderkend.

Het eerste risico is identiteitsfraude[30], vooral in het geval van identificatie en authenticatie. Het biometrische apparaat mag niet worden misleid door een spoofing-aanval en moet verzekeren dat de persoon die een poging doet om de matching uit te voeren, daadwerkelijk de persoon is die staat geregistreerd in het systeem. Die dreiging lijkt minder zinvol te zijn voor biometrische gegevens die niet kunnen worden verzameld zonder de kennis van de betrokkene, zoals aderpatronen. Het is echter een groot probleem voor vingerafdruk- of gezichtsherkenningsapparaten. Vingerafdrukken worden overal achtergelaten door simpelweg het aanraken een object. Het gezicht kan ook worden afgevangen door het nemen van een foto, zonder dat de betrokkene zich daarvan bewust is.

Het tweede risico is het doel afleiding, hetzij door de verwerkingsverantwoordelijke voor de verwerking zelf of door een derde partij onder wie de wetshandhavingsautoriteiten. Deze gemeenschappelijke dreiging met betrekking tot persoonsgegevens wordt van cruciaal belang bij het gebruik van biometrische gegevens. Fabrikanten moeten alle veiligheidsmaatregelen nemen om elk onrechtmatig gebruik van de gegevens te voorkomen en ervoor zorgen dat alle gegevens die niet meer nodig zijn met het oog op de verwerking onmiddellijk worden verwijderd.

Zoals met ieder ander gegeven mogen rechtmatig verwerkte of opgeslagen biometrische gegevens of de bronnen van biometrische gegevens niet door de verwerkingsverantwoordelijke worden verwerkt of ingeschreven voor een nieuw of ander doel tenzij hiervoor een nieuwe legitieme reden is.

Het derde risico is inbreuk op de gegevensbeveiliging, die vereist in de biometrische gegevens context speciale acties afhankelijk van het soort gegevens die zijn gecompromitteerd. Indien een systeem is gebruikt dat biometrische gegevens op een template via een algoritme omzet in een bepaalde code en de biometrische gegevens of het algoritme wordt gestolen of aangetast, moet deze worden vervangen. Wanneer een inbreuk op de gegevensbeveiliging het verlies van direct geïdentificeerde biometrische gegevens betreft die zeer dicht bij de bron van biometrische gegevens liggen, zoals afbeeldingen van gezichten of vingerafdrukken, zal dit aan de betrokken persoon in detail moeten worden gemeld, zodat zij zichzelf kunnen verdedigen in een mogelijke toekomstige gebeurtenis waarbij deze compromitteerde biometrische gegevens tegen hen als bewijs gebruikt zouden kunnen worden.

[29] Dit kan een negatieve impact tot gevolg hebben op het effectueren van rechten van betrokkenen. Inzet van 'cloud computing' op verschillende systeemlagen en door (onder)aannemers in de eID-infrastructuur keten (verschillende subbewerkers, mogelijk verspreid over diverse jurisdicties en continenten) en misbruik van systemen en datalekken. Overnames van in EU gevestigde organisaties die diensten leveren binnen het eID Stelsel door organisaties die gevestigd zijn buiten de EU. Dit met als mogelijk risico dat ook databases worden verplaatst naar andere locaties en onder andere jurisdicties vallen.
[30] Dit risico is vanzelfsprekend ook relevant voor andersoortige identificatie en authenticatiesystemen.

CONTACT

Mazars Management consultants

Jan Matto, partner
T: 088 277 15 09
E: jan.matto@mazars.nl