Grip op Privacy

Handleiding Privacy by Design

"Deze handleiding biedt ontwerpers een bibliotheek met ontwerpkeuzes en oplossingen in het enerzijds formele en anderzijds creatieve proces, om te komen tot een ontwerp dat op een passende wijze invulling geeft aan de privacyvereisten, zoals die in de wet zijn beschreven en in de Privacy Baseline concreet zijn gemaakt."

Status	versie 3.0: update in overeenstemming met de Avg
Auteurs	Marcel Koers, met medewerking van Ruud de Bruijn en bijdragen van leden van de CIP-werkgroep Privacy by design.
Datum	7 mei 2017
Filenaam	20170507 Handleiding Privacy by Design v3_0

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Deze publicatie valt in categorie 2: "becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties". Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site https://cip.pleio.nl.

CIP-documenten kunnen van tijd tot tijd aanpassingen ondergaan of worden ingetrokken als gevolg van veranderde inzichten. De CIP-redactie streeft binnen haar mogelijkheden naar een zo actueel mogelijke status van de documenten. In de praktijk zal enige tijd verstrijken voordat wijzigingen kunnen zijn doorgevoerd. Suggesties voor aanpassingen kunnen ook door lezers worden aangedragen en worden altijd in behandeling genomen.

Bij deze publicatie

Deze editie van de Handleiding Privacy by Design is geënt op de meest recente versie van de Privacy Baseline (v3 en hoger) en is daarmee gebaseerd op de Europese Algemene verordening gegevens-bescherming en de meest actuele conceptversie van de Nederlandse Uitvoeringswet daarbij.

De samenstellers zijn uitgegaan van wat bij het schrijven van de teksten praktisch en volgens de vigerende inzichten en beschikbare kennisbronnen juist werd geacht te zijn. Voortschrijdend inzicht, jurisprudentie en mogelijk aanpassing van de wetgeving zullen hierop in de toekomst aanleiding tot herziening, aanvulling of aanpassing kunnen leiden.

Vooraf

Het kan voor organisaties een uitdaging zijn om op een juiste manier met de persoonsgegevens om te gaan. Wat, waar, door wie en op welke wijze zaken geregeld moeten worden om privacy op een juiste wijze te waarborgen is voor (medewerkers van) organisaties niet altijd duidelijk. Deze Handleiding Privacy by Design (PbD) biedt organisaties handvatten voor een concrete aanpak voor de omgang met privacy bij het ontwerpen van gegevensverwerkingen. Wij kijken naar de gehele gegevensverwerking, dus de verwerking in geautomatiseerde systemen én de handmatige verwerking. Dat laatste betreft de handmatig uitgevoerde bedrijfsprocessen, al dan niet als verlenging van de geautomatiseerde processen. Deze processen zijn te onderscheiden van het 'menselijk gedrag' met betrekking tot privacy. Het menselijk gedrag is meer het domein van wat doorgaans met (privacy)awareness of privacybewustzijn wordt aangeduid. Het accent in deze handleiding zal in het algemeen dus liggen op de bedrijfsprocessen en niet zozeer op het menselijk gedrag.

De samenstellers zijn dank verschuldigd aan Angélique van Oortmarssen, mede-auteur van de eerste editie (2016), en aan de contribuanten van destijds, de leden van de Werkgroep Privacy by Design, met name: Wendie Molendijk (Belastingdienst); Mireille Reiners (Capgemini); Ad Kint (CIP); Bart de Goeij (PMP); Christiaan Hillen (destijds Valori); Dirk Schravendeel (PBLQ); Henk Ameling (Aegon); Ric Gielen (Valori); Wouter Diephuis (Logius).

Wij danken eenieder hartelijk voor de waardevolle bijdragen.

Wijzigingen in versie 3.0

Met de komst van de AVG en de Uitvoeringswet Avg moest de Baseline worden aangepast aan deze gewijzigde privacywetgeving. Tevens is zijn de in de Baseline v3.0 de criteria 'gesaneerd' en is hun aantal teruggebracht tot 13. Omdat deze handleiding is gebaseerd op de Baseline, was alleen om die reden als een update naar v3.0 noodzakelijk. Deze versie gaat uit van de nieuwe Privacy Baseline en de nieuwe privacywetgeving (eventuele sectorspecifieke wet- en regelgeving uitgezonderd).

Amsterdam, 7 mei 2017

Over CIP

CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheids-organisaties. Het heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waarin ook gespecialiseerde marktorganisaties als kennispartners deelnemen.
Het centrum is opgericht voor informatieuitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening. Inmiddels bestaat het CIP-netwerk uit een groot aantal overheidsorganisaties en (private) kennispartners. Kennis die in deze organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt.

Het produceren van themadocumenten op basis van inbreng vanuit het netwerk is er één van. Aangesloten organisaties leren van elkaars oplossingen en werkwijzen en kunnen samen komen tot afspraken daaromtrent. Door meer samen doen draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen. De producten van het CIP worden om niet ter beschikking gesteld.

Managementsamenvatting

Privacy bij de kop vatten zoals organisaties ermee moeten werken en waarop zij worden gecontroleerd. Dit is wat de documenten in de CIP reeks *Grip op privacy* faciliteren. Organisaties (zowel publiek als privaat) hebben rekening te houden met de privacy van betrokkenen wanneer zij 'iets' doen met persoonsgegevens. 'Iets' kan van alles zijn: alleen al het ontvangen of inzien van persoonsgegevens valt al onder 'het verwerken' ervan, waarop de privacywet- en regelgeving van toepassing is.

Werken met persoonsgegevens noodzaakt organisaties werk te maken van 'informationele privacy'. Dit is de bescherming van personen in verband met informatie die over de persoon bekend is en ten aanzien van de persoon wordt toegepast, ook wel bescherming van persoonsgegevens (of: gegevens-bescherming) genoemd. Het recht op bescherming van persoonsgegevens is verankerd in de Grondwet en internationale mensenrechtenverdragen. Regels over hoe om te gaan met dit grondrecht zijn verankerd in de Europese Algemene verordening gegevensbescherming (Avg), de Nederlandse Uitvoeringswet Avg, en sectorspecifieke wetgeving (zoals de bijvoorbeeld de Telecommunicatiewet en de regels voor financiële instellingen).

Een van de uitgangspunten van de Avg is dat iedereen de mogelijkheid moet hebben om na te gaan waar zijn persoonsgegevens worden vastgelegd en verwerkt, waarom en door wie. De betrokken organisatie en haar eventuele ketenpartners moeten daarin voorzien. Er is bovendien een correctierecht geregeld en een 'recht op vergetelheid'.
Dat lijkt een blok aan het been, maar dat hoeft het niet te zijn wanneer je er van begin af aan rekening mee kunt houden. Achteraf aanpassen of 'bijplakken' is kostbaar en leidt vaak tot inefficiënte, suboptimale resultaten.

Privacy by Design gaat over proactieve maatregelen in plaats van reactieve, anticiperen op en voor-komen van inbreuken op iemands privacy voordat deze plaatsvinden. PbD verkleint niet alleen de kans op privacyschending, maar ook het risico van boetes en schadeclaims.

Na een algemene introductie van de drie ACT-doelen: Afscherming, Corrigeerbaarheid en Transparantie. voor de omgang met persoonsgegevens, worden in deze handleiding de daarbij passende concrete maatregelen besproken die de organisatie kan implementeren - en bij voorkeur dus al in de ontwerpfase kan meenemen - om systematisch aan de vereisten voor gegevensbescherming te voldoen.
De handleiding biedt daarvoor:

- Een aanpak om de complexiteit van PbD te reduceren;
- Een lijst met principes die nuttig zijn om aan de ACT-doelstellingen te kunnen voldoen;
- Principes, waarover bewust een ontwerpbeslissing genomen kan worden;
- Uitleg bij de principes in combinatie met technologieën die kunnen worden gebruikt.

Wij denken dat deze handleiding niet alleen goede diensten kan bewijzen aan ontwerpers van software. Procesontwerpers en business analisten, managers die betrokken zijn bij ontwerptrajecten (software en processen) en inkopers kunnen eveneens baat hebben bij deze handleiding.

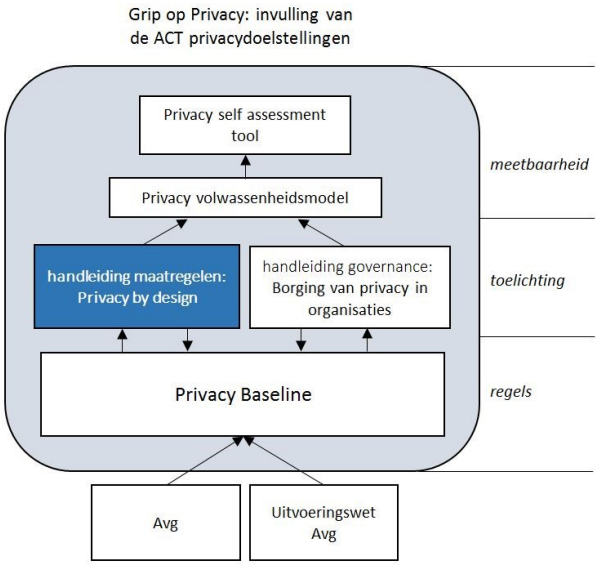
De Avg is op 25 mei 2016 van kracht geworden en staat een implementatieperiode toe tot 25 mei 2018. Wachten met het inregelen van privacymaatregelen binnen de organisatie en met uw ketenpartners tot aan dat moment is bepaald niet raadzaam en was al niet conform de Wet bescherming persoons-gegevens. De kernbeginselen van informationele privacy, zoals doelbinding, dataminimalisatie en kwaliteit van gegevens komen in de Avg onverkort of zelfs strenger terug en overtredingen kunnen aanmerkelijk hoger worden beboet.

Er ligt ook een bonus in het verschiet: toepassen van Privacy by Design verhoogt de kwaliteit van de gegevensverwerking en daarmee de kwaliteit van dienstverlening en het imago van de organisatie.

Over Grip op privacy

Deze handleiding hoort in een set van samenhangende documenten onder de noemer 'Grip op privacy':

- Privacy Baseline
- Privacy by Design
- Privacy Governance
- Het Privacy Volwassenheidsmodel
- Het Privacy Self Assessment



De *Privacy Baseline* vertaalt de privacywetgeving naar concrete, hanteerbare normen die duidelijk aangeven waar organisaties wat moeten regelen in hun privacybeleid, de uitvoering en de controle erop; de Privacy Baseline biedt concrete handvatten voor de juiste omgang met persoonsgegevens

De *twee handleidingen* betreffen de toepassing van de juiste maatregelen en de inrichting van de organisatie waarmee 'Grip op privacy' op de meest efficiënte en effectieve wijze kan worden bereikt. Het zijn toelichtende verhandelingen over:

- Hoe je kunt bewerkstelligen dat het aspect privacy van begin af aan in de ontwikkeling van programmatuur wordt meegenomen (by design).
- Hoe je privacy in alle relevante bedrijfsprocessen implementeert, borgt, kunt onderhouden en verbeteren (governance).

Bij de Baseline hoort een speciaal daarop gebaseerd *Privacy volwassenheidsmodel*. Door privacy actief te hanteren als kwalitatief element in de bedrijfsvoering, kunnen organisaties privacy benutten om de dienstverlening aan de klanten op een hoger peil te brengen en zo naar een hoger niveau van volwassenheid te komen. Dit aspect wordt ter hand genomen in het document 'Privacy Volwassenheids-model', een praktische handleiding voor het vaststellen en vergroten van de organisatievolwassenheid in relatie tot de omgang met persoonsgegevens.
Het Privacy volwassenheidsmodel is tevens een referentiemodel, afgeleid van gangbare 5-laagse volwassenheidsmodellen. Het specificeert de niveaus op het aspect van privacy. De 5 niveaus worden gedefinieerd aan de hand van de mate waarin je voldoet aan de Privacy Baseline.
Hoe volwassen gaat de organisatie met privacy om? Welk niveau wil de organisatie nastreven en wat is daarvoor nodig? Op deze vragen geeft het *Privacy self assessment tool* antwoorden. Het geeft aan wat je nog te doen staat om het (aan het begin zelf gekozen) volwassenheidsniveau te bereiken.

De methode Grip op privacy biedt zo concrete handvatten om de juiste omgang met persoonsgegevens te bewerkstelligen, te waarborgen en het privacybeleid passend, effectief en efficiënt in te passen in de bedrijfsvoering. Het gaat niet om de normen. Het gaat erom de ACT principes: Afscherming, Corrigeer-baarheid en Transparantie te realiseren en daarmee maximaal de betrokkene te respecteren in zijn privacy. Dit wordt verderop in het document uitgebreid behandeld.

Draagvlak door brede inbreng uit het CIP-netwerk

De methode 'Grip op Privacy' en de afzonderlijke documenten daarvan zijn tot stand gekomen door nauwe samenwerking met en tussen verschillende partijen in het CIP-netwerk. De auteurs danken alle CIP-ers, geïnterviewde deskundigen, leden van de CIP Domeingroep Privacy, de Werkgroep Pb2Avg en de Werkgroep Privacy By Design, die een bijdrage hebben geleverd aan het samenstellen van de methode. Hun bijdragen en het gegeven dat een breed palet van organisaties hen daartoe in staat stelt, geven de auteurs het vertrouwen dat de methode 'Grip op privacy' voldoende draagvlak heeft voor een brede toepassing en verdere ontwikkeling.

Inhoud

1 Inleiding

Eind 2014 kreeg CIP uit de CIP community de vraag om eens op te schrijven "hoe dat nou moet, met die privacy". De vraag was niet uit voortgekomen uit naïviteit, maar uit de wirwar aan informatie en opvattingen over privacy.
Het antwoord hebben we gezocht in de pragmatiek: pak privacy bij de kop zoals organisaties en bedrijven ermee zouden moeten werken. Daarvoor gelden immers wetten en voorschriften en de discussie over óf het moet en wát er moet is dus al gepasseerd. De Avg inclusief de Uitvoeringswet Avg en het daarbij horende Memorie van toelichting (Mvt) vormen de geldende privacykaders en wat je er ook van vindt, daaraan heb je als bedrijf of organisatie te voldoen[1,2].

Informationele privacy als uitgangspunt
Organisaties kunnen ervoor kiezen om 'slechts' te voldoen aan de wet. Maar Privacywetgeving is niet uitsluitend een hinderpaal. Door verantwoord en efficiënt om te gaan met de balans tussen wetgeving, de taakstelling van de organisatie en de persoonlijke levenssfeer van betrokkenen, is 'privacy' ook als een kwaliteitskenmerk ten voordele te benutten. Er zijn al commerciële bedrijven die hun privacybeleid bewust in hun marketing etaleren. Overheidsorganisaties moeten in dit opzicht bij uitstek het goede voorbeeld geven.

Een organisatie die transparant en concreet wil zijn over haar privacybeleid, en ook netjes wil voldoen aan de wettelijke vereisten om boetes, imagoschade en schadeclaims te voorkomen, moet proactief werk maken van het type privacy dat informationele privacy wordt genoemd.

Informationele privacy gaat over bescherming van personen in verband met informatie die van of over hen bekend is en/of ten aanzien van hen wordt toegepast[3]. Dit wordt ook wel bescherming van persoonsgegevens (of: gegevensbescherming) genoemd en is verankerd in de Grondwet[4] en verder uitgewerkt in de Avg en de Uitvoeringswet Avg.

Deze handleiding Privacy by Design 3.0. gaat over hoe je kunt bewerkstelligen dat het informationele privacy van begin af aan in de ontwikkeling van programmatuur wordt meegenomen (by design).

Voor wie?
Anders dan de titel mogelijk doet vermoeden, is deze handleiding niet alleen bedoeld voor ontwerpers van software. Procesontwerpers en business analisten kunnen net zo goed profiteren van de 'by design principes'. Dat zo zijnde kunnen wij ons voorstellen dat ook de managers die betrokken zijn bij ontwerptrajecten (software en processen) en inkopers baat kunnen hebben bij deze handleiding.

De principes voor het Privacy by Design proces zijn beschreven in hoofdstuk 2. Zij appelleren aan de houding van de ontwerpers. De daarop volgende hoofdstukken gaan over het ontwerp zelf en beschrijven de principes en de door de ontwerper - samen met de proceseigenaar - te maken ontwerpkeuzes. Hoofdstuk 3 behandelt de afweging of persoonsgegevens mogen worden verwerkt.
De Privacy Baseline geeft de criteria voor de inrichting van de verwerking, maar beschrijft niet hoe je die toepast: dat is het onderwerp van hoofdstuk 4. Waarna de hoofdstukken 5 - 7 in nader detail ingaan op de realisering van de vereisten en principes. Hoofdstuk 8 ten slotte gaat over de afwegingen en maatregelen die nodig zijn voor een veilige verwerking van persoonsgegevens op (mobiele) apparaten die niet in een afgeschermde werkomgeving worden gebruikt.

---

[1] Wij verwijzen naar deze Uitvoeringswet plus het Mvt als: de Uitvoeringswet Avg. We wijzen erop dat ten tijde van schrijven de Uitvoeringswet nog een concept is - wij hanteren de conceptversie van april 2017.
[2] Bedrijven en organisaties: wij hanteren 'organisatie' voor beide aanduidingen in de publieke en private sectoren.
[3] S. Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet*, SDU Uitgevers, Den Haag, 2005, p.19.
[4] Art. 10 lid 2 van de Grondwet.

2 Privacy by design

Aanpassen achteraf is moeilijker en kostbaarder dan van begin af aan inbouwen. Dat geldt ook voor het inbouwen van maatregelen en processen die privacy bewerkstellingen.

2.1 De Privacy by Design doelstelling

De doelstelling van Privacy by Design is verwoord in de definitie ervan:

> *Het inbedden van de privacycriteria (met de Privacy Baseline als basis) in de ontwerpen en het beheer (van delen) van informatiesystemen, en het inbedden van de privacymaatregelen in de technologie.*
> *Dit is inclusief de begeleiding van de ontwerpers en de beheerders bij de keuzes die gemaakt moeten worden, zodat privacy in een vroeg stadium wordt verankerd in de concretisering van informatie-behoefte en het ontwerp.*

Privacy by Design (PbD) is daarmee een proactieve benadering van de bescherming van privacy door het meenemen van privacy in het ontwerp van een technische voorziening voor de verwerking van persoonsgegevens. PbD is meer dan alleen de technische keuzes. De techniek wordt ingezet om de privacyprocessen te vereenvoudigen en te borgen. Soms door de processen te automatiseren en soms door functionaliteit te bieden of de juiste informatie aan te leveren aan de privacy-processen. Privacy by Design betekent dat systeemarchitecten, ontwerpers en ontwikkelaars de privacycriteria, zoals die in de Privacy Baseline zijn beschreven, meenemen of ten minste meewegen in wat zij opleveren.

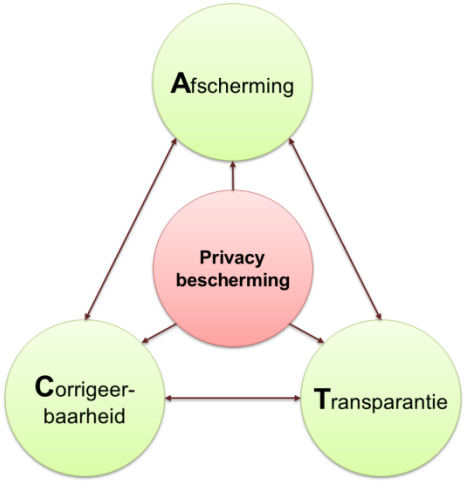
Dit kan eenvoudig procedureel worden ingebed in de maakprocessen door impact op de privacy mee te nemen bij alle nieuwe ontwerpen, net zoals dat inmiddels geldt of zou moeten gelden voor Security by Design (SbD). PbD is in het belang van de organisatie, alleen al omdat het inbouwen van maatregelen in een latere fase vele malen duurder is. De Algemene Verordening weerspiegelt het groeiende belang dat aan privacy wordt gehecht door Privacy by Design verplicht te stellen voor alle organisaties die met persoonsgegevens werken.[5]

2.2 Afscherming, corrigeerbaarheid en transparantie: ACT

De Privacy Baseline beschrijft de criteria waaraan de verwerking van persoonsgegevens moet voldoen. Dit heeft gevolgen voor het ontwerpproces van verwerkingen. Door decompositie van een verwerking, zoals in de Privacy Baseline is gehanteerd, wordt duidelijk waar (binnen de verwerking) wat (aan ontwerpeisen) moet worden ingevuld om aan de ACT-privacy-eisen te voldoen. Het resultaat moet zijn dat de ACT doelen worden gehaald. Deze zijn als volgt gedefinieerd:

Afscherming: Afscherming zorgt ervoor dat persoonsgegevens niet op een onrechtmatige manier kunnen worden verwerkt, zoals het gebruiken, doorgeven of koppelen van persoonsgegevens voor andere doelen dan de oorspronkelijke of voor onbekende doeleinden.

Corrigeerbaarheid: Tijdens en na elke verwerking van persoons-gegevens is het mogelijk om de persoonsgegevens en de uitkomsten van de verwerking aan te passen, indien deze niet voldoen aan de doelbinding of de kwaliteitsvereisten en daardoor de betrokkene (kunnen) benadelen.



[5] In de Nederlandse vertaling van de AVG, overweging 78, wordt gesproken van maatregelen toepassen "die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen."; dit vindt zijn weerslag in Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen.

Transparantie: Voor, tijdens en na elke verwerking van persoonsgegevens bestaat duidelijkheid over de gehele gegevensverwerking, waaronder het doel, de wettelijke grondslag en de organisatorische en technische inrichting van verwerking van de persoonsgegevens.

Privacy by Design is opgesteld om een aanpak en handvatten in de vorm van principes te bieden die de complexiteit van het ontwerp, waarmee de ontwerper wordt geconfronteerd bij het inbouwen van privacy, reduceren. PbD biedt daarvoor:

- Een lijst met principes die nuttig zijn om aan de ACT-doelstellingen te kunnen voldoen.
- Principes, waarover bewust een ontwerpbeslissing genomen kan worden.
- Uitleg bij de principes in combinatie met technologieën die kunnen worden gebruikt.

Deze handleiding PbD biedt zo de ontwerpers een bibliotheek met ontwerpkeuzes en oplossingen in het enerzijds formele en anderzijds creatieve proces, om te komen tot een ontwerp dat op een passende wijze invulling geeft aan de privacyvereisten, zoals die in de wet zijn beschreven en in de Privacy Baseline concreet zijn gemaakt. Deze handleiding PbD is daarmee nadrukkelijk niet bedoeld voor het benoemen van alle technieken die bestaan voor het beschermen van de privacy. Deze technieken worden overigens aangeduid als Privacy Enhancing technologies (PET's).

2.3 Privacy by Design binnen bestaande ontwerpmethoden

Het waarborgen van de vereisten van de Privacy Baseline is een continu en cyclisch proces. Veranderingen in het beeld van wat passende maatregelen zijn, nieuwe bedreigingen, incidenten of een veranderende wet- en regelgeving kunnen leiden tot een heroverweging van de genomen maatregelen en ontwerpbeslissingen. Op bedrijfsniveau gebeurt dit binnen het *governanceproces*.

Op *projectniveau* moet het waarborgen van de vereisten een proces zijn dat integraal onderdeel uitmaakt van het ontwerpproces. Het maakt daarbij niet uit of ze toegepast worden in een lineair ontwerpproces, zoals bijvoorbeeld de watervalmethode, of in een cyclisch ontwerpproces, zoals bij het Agile ontwikkelen.
De watervalmethode is een aanpak met vast omlijnde fases. Iedere fase volgt de andere op met vastgelegde eisen. Dit in tegenstelling tot de meeste agile-methoden die proberen risico's van verkeerde eisen te verminderen door het systeem en de software te ontwikkelen in korte overzichtelijke perioden (timeboxes), die 'iteraties' genoemd worden.

In het lineaire proces worden de privacyvereisten meegegeven aan het begin van het ontwerpproces. De vereisten zijn dan op basis van een risicoanalyse of gegevensbeschermingseffectbeoordeling (GEB)[6] in principe eenmalig bepaald en ingebracht. Bij een cyclisch ontwikkelproces is aan het begin nog niet zo duidelijk wat het systeem precies gaat doen. Dit wordt gaandeweg bepaald in de opeenvolgende iteraties van het cyclische proces. Een iteratie wordt daarbij aangeduid als 'sprint'. Hierdoor is het meegeven en bewaken van de eisen complexer en worden bepaalde stappen, zoals de risicoanalyses, uitgesmeerd over meerdere sprints. De eisen zelf, zoals die in de Privacy Baseline zijn beschreven, zijn productonafhankelijk en kunnen daardoor dus aan de start van een ontwikkelproces worden ingebracht. De wijze waarop de eisen binnen de sprints moeten worden ingevuld - en daarmee ook het detailniveau van de eisen - is wel verwerkingsafhankelijk.

2.4 De 7 principes van Privacy by Design

Het doel van Privacy by Design ligt in lijn met het doel van de methode Grip op Privacy, zijnde voor individuele personen (betrokkenen) het verzekeren van zicht op en zo mogelijk controle over de eigen persoonsgegevens en voor organisaties het verkrijgen en behouden van een positie binnen de markt van het aanbieden van diensten, waarbij persoonsgegevens verwerkt worden. Dit is mogelijk door het toepassen van 7 leidende principes voor PbD. Zij zijn afgeleid van de 7 fundamentele principes die zijn opgesteld door de Information and Privacy Commissioner van Ontario in Canada.[7]

[6] Voorafgaand aan de Avg was dit het Privacy Impact Assessment (PIA)
[7] Strong Privacy Protection - Now, and Well into the Future, 2011) [1].

2.4.1 Proactief en preventief in plaats van reactief en herstellend

Privacy by Design kenmerkt zich door het nemen van proactieve maatregelen in plaats van reactieve. Het anticipeert op en voorkomt inbreuken op iemands privacy voordat deze feitelijk plaatsvinden. PbD wacht niet totdat de privacydegradatie een feit is. PbD biedt zij oplossingen voor privacydegradatie die reeds heeft plaatsgevonden. Tenzij PbD actueel wordt bij een grote wijziging van de gegevensverwerking, moet privacydegradatie tijdens de levensduur van een verwerking worden voorkomen door het periodiek uitvoeren van een GEB. Het doel van PbD is om te voorkomen dat privacy onvoldoende aandacht krijgt bij de bouw of bij een (grote) aanpassing van de gegevensverwerking. Met PbD wordt niet alleen privacydegradatie of de kans daarop verkleind, maar ook het risico van imagoschade, boetes en schadeclaims .

Leidend PbD principe 1
Privacy by Design geldt vanaf de initiatie van het ontwerp en niet achteraf. Starten met Privacy by Design start al bij de beleidsvorming.

Privacy by Design is daarmee meer dan het meenemen van privacy vanaf het ontwerp van een systeem of, breder gesteld, de gegevensverwerking. PbD start al op organisatieniveau bij de beleidsvorming (B.01).

2.4.2 Privacy by default

Van één ding kunnen we zeker zijn: de standaard is de regel. PbD streeft naar een maximale privacy door te verzekeren dat persoonsgegevens in een IT-systeem of handelingspraktijk de privacy *automatisch* afdoende beschermd is. Ook als het individu zelf niets onderneemt zal toch zijn privacy zijn gewaarborgd. Van het individu wordt geen specifieke actie gevraagd om zijn privacy te beschermen, dat is standaard ingebouwd in het systeem. PbD is in de Avg een vereiste.[8]

Leidend PbD principe 2
Privacycriteria gelden per default. Daarbij is de regel: "comply or explain".

Voor alle maatregelen geldt dat deze passend moeten zijn en er dus rekening gehouden kan worden met de risico's, de stand van de techniek, de uitvoeringskosten en de omvang en aard van de verwerking. Tegelijkertijd staat het belang van de betrokkenen centraal, zoals ook beschreven wordt in PbD principe 7. Bij de afweging in welke mate een maatregel of een criterium wordt gehanteerd is het belang van de betrokkene leidend. Hierbij wordt gekeken naar de 'invloed' op de persoonlijke levenssfeer.

> Het begrip ''invloed'' is breed. Het schenden van de privacy door het niet vertrouwelijk omgaan met de perspoonsgegevens en het verwerken van onjuiste persoonsgegevens vallen daar bijvoorbeeld onder. Echter ook het verhogen van de kosten van een dienst aan de betrokkenen, door het nemen van niet-passende c.q. te dure maatregelen, kunnen daar onder vallen. Juist dit is een van de afwegingen die bij "comply or explain" moeten worden meegenomen.

2.4.3 Privacy geïntegreerd in het ontwerp

PbD is geïntegreerd in het ontwerp en de architectuur van IT-systemen en handelingspraktijken. Het is er niet als een extraatje of een lastig los onderdeel aan vastgeplakt, bijvoorbeeld nadat er een privacyschending heeft plaatsgevonden of zwakke plekken zijn ontdekt. Als resultaat hiervan is privacy een essentieel onderdeel van de kernfunctionaliteit. Privacy is geïntegreerd in het systeem, zonder aan functionaliteit in te moeten leveren.

[8] Art. 25, Avg

Leidend PbD principe 3
Privacymaatregelen zijn integraal onderdeel van de informatieverwerking en zijn geen add-on. Dit geldt voor de technische systemen én de organisatorische processen.

Door privacymaatregelen integraal mee te nemen in de organisatorische processen, in het functioneel ontwerp en vervolgens in het technisch ontwerp, kun je de meerkosten voor privacy beperkt houden. Reparatie achteraf is doorgaans altijd duurder. Separaat ontwikkelde toevoegingen zijn van zichzelf al duurder dan generiek meegenomen toepassingen en vragen om koppelingen met bestaande functionaliteit die alsnog leiden tot aanpassingen van die bestaande functionaliteit. Het gevaar is dan bovendien dat deze meerkosten kunnen leiden tot discussie over de noodzaak versus de proportionaliteit van deze aanvullende maatregelen. Dit gezien de kosten en complexiteit ervan.

2.4.4 Volledige functionaliteit – win/win in plaats van compromissen

Privacy by Design streeft ernaar om alle legitieme belangen en doelstellingen op de wijze van een 'win-win' te faciliteren, en niet op ouderwetste wijze met elkaar te verzoenen door middel van compromissen waar die niet nodig zijn. PbD voorkomt dat schijnbaar tegengestelde belangen (bijvoorbeeld doordat privacy en veiligheid of privacy en snelle dienstverlening) tegen elkaar worden uitgespeeld. Door win-win te faciliteren kan worden gedemonstreerd dat een combinatie van beiden wel degelijk mogelijk is.

Leidend PbD principe 4
Het waarborgen van de privacy is een verantwoordelijkheid van alle betrokkenen partijen. Het is niet een add-on op de criteria voor één partij.

Privacy is niet iets wat een Functionaris voor de Gegevensbescherming of een bepaald persoon wil. Door het belang van privacy door eenieder te laten onderkennen, bijvoorbeeld door het creëren van privacybewustzijn in awareness trainingen, wordt privacy een gedeelde verantwoordelijkheid. Bedenk dat zonder een collectief bewustzijn de andere principes ook makkelijk onderuit gehaald kunnen worden.[9] Je kunt privacy nog zo goed inregelen, als het besef ontbreekt bij de mensen die het moeten ondersteunen dan kan dat andere principes gemakkelijk teniet doen.

2.4.5 Bescherming tijdens de volledige levenscyclus

Krachtige veiligheidsmaatregelen zijn essentieel voor het behoud van privacy, van begin tot eind. Privacy by Design, geïntegreerd in een systeem nog voordat er enige informatie is verzameld, strekt zich uit over de gehele levenscyclus van de betrokken gegevens. Alleen zo heb je de garantie dat alle gegevens op een veilige wijze zijn verkregen en op een tijdige en veilige wijze zijn vernietigd aan het eind van het proces. Zodoende verzorgt PbD een juiste behandeling van gegevens en een veilige omgang met informatie van begin tot eind.

PbD: Leidend principe 5
Privacy by Design waarborgt het privacymanagement, inclusief de beveiliging, gedurende de gehele levenscyclus van de persoonsgegevens. Het is niet een eenmalige actie.

Verwerkingen van persoonsgegevens kunnen in de loop van de tijd wijzigen. Bij het ontwerpen van systemen moet daarom rekening gehouden worden met veranderende omstandigheden. Hiervoor is het nodig dat de

[9] Op het vergroten van het verandervermogen wordt ingegaan in "Borgen van Privacy in Organisaties" van het CIP. Hierin wordt ingegaan op hoe de kracht van de organisatie benut kan worden om grip op privacy te krijgen.

werking van de privacymaatregelen gemonitord kan worden (ten behoeve van zichtbaarheid en transparantie) en dat het ontwerp veranderingen gemakkelijk aan kan. Deze veranderbaarheid start al bij de architectuurkeuzes in het ontwerp en zelfs nog wel eerder: als bewust gekozen vereiste in het beleid. Door te voldoen aan het stelsel van criteria uit de Privacy Baseline (Beleid, Uitvoering en Controle) wordt de gehele levenscyclus, inclusief de benodigde governance, afgedekt.

2.4.6 Zichtbaarheid en transparantie – hou het open

Privacy by Design streeft ernaar om alle belanghebbenden, bij welke technologie of handelingspraktijken dan ook, ervan te verzekeren dat het systeem feitelijk opereert conform de oorspronkelijk geclaimde beloftes en doelstellingen, dit geheel ter verificatie door onafhankelijke derden. De technische componenten en het operationeel handelen blijven zichtbaar en transparant voor zowel de gebruikers als de dienstverleners. Onthoud: vertrouwen is de basis, maar nooit zonder controle.

Leidend PbD principe 6
Inzicht en transparantie over hoe persoonsgegeven worden verwerkt moet mogelijk zijn voor zowel de betrokkene persoonlijk, als "eenieder, de eigen organisatie en toezichthouders".

Inzicht en transparantie over hoe persoonsgegevens worden verwerkt is binnen de wet- en regelgeving een criterium en moet mogelijk gemaakt worden voor de betrokkene, eenieder, de eigen organisatie en toezichthouders. Zie hiervoor de criteria C.01 en C.02 in de Privacy Baseline.

2.4.7 Respect voor de privacy – laat de gebruiker centraal staan

Privacy by Design heeft boven alles architecten en exploitanten nodig die de belangen van het individu als hoogste prioriteit beschouwen en deze overtuiging toepassen door maatregelen in te stellen zoals krachtige privacy instellingen, passende informatievoorziening en gebruikersvriendelijke opties. Zij stellen de betrokkene te allen tijde centraal.

Leidend PbD principe 7
Technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van de betrokkenen beschermen.

Het toepassen van technologieën is slechts een middel. PbD heeft zijn doel pas bereikt, wanneer het (binnen de context van de verwerking van persoonsgegevens) daadwerkelijk zorg draagt voor de bescherming van de persoonlijke levenssfeer. Niet het toepassen of uitvoeren van een maatregel is hierbij leidend, maar de beoogde betekenis voor de betrokkene. Bij iedere maatregel moet daarom verder gekeken worden dan alleen het uitvoeren ervan: er moet vastgesteld worden of het beoogde resultaat voor de betrokkene zich daadwerkelijk voordoet. Het correctierecht, het laten staken van de verwerking van zijn of haar gegevens en het uitwissen van de gevolgen voor de persoonlijke levenssfeer van de betrokkene zijn voorbeelden, waarbij de persoonlijke levenssfeer kan worden beschermd. Implementatie van criterium U.03 en de uitwerkingen daarvan in paragraaf 6.2 kunnen als een belangrijk vereiste om dit principe te waar te maken

2.5 Privacy by Design en Privacy Enhancement Technologieën

Privacy Enhancement Technologieën (PET) worden vaak in één adem genoemd met Privacy by Design. PbD is echter een aanpak en PET een lijst met technologieën. Bovendien kennen ze een verschillend aandachtsgebied.

2.5.1 Privacy Enhancement Technologieën

Privacy Enhancement Technologieën zijn te verdelen in 2 vormen van *technische hulpmiddelen die de privacymaatregelen ondersteunen*:

1. **Ondersteuning van de organisatorische processen**:
   Hieronder vallen de hulpmiddelen die de administratieve processen in de Privacy Baseline ondersteunen. PET in deze vorm geeft met name invulling aan de criteria voor het domein Beleid en voor Control/Beheer in de Baseline. Deze hulpmiddelen worden, waar relevant, genoemd in de Handleiding Borgen van Privacy in organisaties van het CIP.
2. **Ondersteuning binnen de technische gegevensverwerking**:
   Dit zijn de voorzieningen die ingebed worden in de systemen. Zij moeten daarom meegenomen worden bij het ontwerp van de technische gegevensverwerking. Veel van deze voorzieningen worden al toegepast in de informatiebeveiliging, zoals bij versleuteling van gegevens en logische toegangsbeveiliging. Deze vorm van PET geeft met name invulling aan de criteria voor het domein Uitvoering en wordt daarom behandeld in deze handleiding.

2.5.2 Privacy by Design in de levenscyclus van de verwerking

PbD gaat verder dan de ontwerpfase en komt voor in alle fasen van de levenscyclus van de verwerking. Ieder fase vraagt om aandacht voor privacy. Daarbij kan in iedere fase binnen de levenscyclus gekeken worden naar de verschillende criteria uit de Privacy Baseline:

3. Initiatie: doelbinding en noodzaak:
   a. Wil/moet ik persoonsgegevens verwerken (U.01)?
   b. Kan ik deze verwerking rechtvaardigen op een grond van de Avg (U.01)?
   c. Is vernietiging of anonimisering persoonsgegevens direct na verwerking mogelijk (U.06)?
4. Informatieanalyse:
   a. Welk niveau van gegevensbescherming moet worden gerealiseerd gezien de risicoanalyse (B.03) en categorie van gegevens (U.01) en de ambities, zoals beschreven in het privacybeleid (B.01)?
   b. Welke verwerwerkingsprocessen vragen om welke informatie (en koppeling) van de gegevensverwerkingen (U.01) en wat is de samenhang tussen de verschillende aspecten, ofwel hoe ziet de gegevensverwerking er uit (U.02)?
   c. Welke technische maatregelen leveren een toegevoegde waarde ten opzichte van organisatorische maatregelen of zijn ondersteunend aan de organisatorische maatregelen?
   d. Wordt de bescherming reeds gewaarborgd door reeds gedefinieerde technische maatregelen, bijvoorbeeld die voor Informatiebeveiliging (zie ook Handleiding Borgen van Privacy in organisaties)?
5. Zijn de verantwoordelijkheden helder (B.02)?
6. Basisontwerp:
   a. Welke gegevens worden verwerkt en op welke grond (U.01)
   b. Hoe lopen de gegevensstromen in het informatiesysteem (U.02)?
   c. Kan de inhoudelijke kwaliteit van de gegevens worden gecontroleerd en aangepast (U.03)?
   d. Hoe worden de betrokkenen ingelicht (U.05)?
   e. Wat is het gegevensmodel voor iedere gegevensstroom in het verwerkingsproces van verzamelen, opslaan, bewaren tot aan vernietigen (U.02 en U.06)?
   f. Welke koppelingen met andere systemen en instanties zijn in ketenverband aanwezig en welke gronden zijn daarvoor (B.01 en U.07)?
   g. Welke voorzieningen zijn er om de juistheid en nauwkeurigheid van persoonsgegevens te bewaken (U.03)?
   h. Welke voorzieningen zijn er zodat de betrokkene persoonsgegevens kan laten corrigeren of overgedragen te krijgen (U.03)?

   i. Leveren de privacymaatregelen de juiste informatie ten behoeve van toezicht en toegang (criteria C.01 en C.02)?
   j. Is een rapportage in geval van een datalek mogelijk (C.03)?
7. Detailontwerp:
   a. Welke beveiligingseisen worden aan de technische maatregelen gesteld (criteria B.02 en U.04)?
   b. Hoe worden de technische maatregelen geïntegreerd in het volledige technisch ontwerp van het informatiesysteem (leidend PbD principe 3)?
8. Ontwikkeling:
   a. Moet de gekozen technische maatregel zelf worden ontwikkeld of zijn er standaardoplossingen beschikbaar (zoals bestaande PET-oplossingen)?
9. Testen:
   a. Functioneren de technische en organisatorische maatregelen op een juiste wijze als onderdeel van het gehele informatieverwerking (leidend PbD principe 3)?
   b. Voldoen de geïmplementeerde technische maatregelen aan de eisen voor gebruikersvriendelijkheid?
   c. Hoe vindt anonimiseren plaats (en hoe is het meegenomen in het ontwerp) of hoe vindt op een andere wijze de bescherming van de persoonsgegevens plaats?[10]
10. Implementatie:
   a. Verandert de werkwijze voor gebruikers door de toepassing van de technische maatregelen en hoe worden gebruikers hierover ingelicht?
   b. Moeten betrokkenen, waarvan de persoonsgegevens worden verwerkt, worden ingelicht (U.05)
   c. Moeten beheerders en gebruikers getraind worden in de toepassing van de technische maatregelen?
11. Beheer en onderhoud:
   a. Welke specifieke privacy-beheeractiviteiten moeten worden uitgevoerd in aanvulling op de reguliere beheeractiviteiten?
12. Evaluatie:
   a. Zijn de privacy maatregelen effectief (leidend PbD principe 7)?
   b. Is een audit of een certificering van het informatiesysteem gewenst (leidend PbD principe 3)?
   c. Wat zijn de gebruikers- en beheerderservaringen?

Bij PbD wordt gekeken naar de gehele gegevensverwerking, dus de geautomatiseerde verwerking in geautomatiseerde systemen én de handmatige verwerking. Zo waarborg je dat eventuele handmatige processtappen in de verwerking van persoonsgegevens worden meegenomen in de privacybescherming. Het accent zal echter vooral liggen op de geautomatiseerde systemen, ofwel 'het informatiesysteem'.

2.6 Privacywetgeving voor nieuwe technologieën

De privacywetgeving loopt al snel achter bij nieuwe technologieën (zoals big data-analysetools en de Internet-of-things), omdat bestaande privacywetgeving geen duidelijke antwoorden heeft of eerst een grondige interpretatie vereist van de nieuwe technologieën. Daarbij is wetgeving is nu eenmaal (veel) trager dan de technologische ontwikkelingen die almaar sneller gaan. Als na verloop van tijd nieuwe wetgeving wordt aangenomen, dan is de nieuwe techniek alweer doorontwikkeld, waardoor nieuwe privacy issues kunnen zijn ontstaan.

Natuurlijk is het nodig om sneller te kunnen reageren op nieuwe technologieën. Maar nog beter is het om bij de ontwikkeling van nieuwe technologieën Privacy by Design mee te nemen. Kijk hierbij vooral naar de toepassingsmogelijkheden en de veranderende verwachtingen van de gebruikers. Vooraf afstemmen met wetgevers kan voorkomen dat complicerende wetgeving ontstaat.

[10] Zie bijv. De CIP publicatie "Testen met persoonsgegevens"

3 Ontwerpen van de gegevensverwerking

Een gegevensverwerking *ontwerpen*? Jazeker, dat is niet zo raar als het misschien klinkt. We hebben het niet over een ledenbestand van de tennisvereniging, maar over een gegevensverwerking waar grote aantallen persoonsgegevens door geraakt worden, en waar andere organisaties en individuen van afhankelijk zijn. Niet alleen moet je rekening houden met wet- en regelgeving, ook de kwaliteit en de robuustheid van de verwerking is van groot belang. En dan ben je er nog niet: de groei van het privacybewustzijn maakt extra aandacht noodzakelijk voor zowel de afscherming als de toegankelijkheid van de gegevensverwerking. Deze zaken betreffen het ontwerp van de software en van de verwerkingsprocessen in de organisatie. Het verwerken van persoonsgegevens omvat alles wat je met persoonsgegevens (van een ander) doet. Het is niet alleen 'muteren', ook 'bewaren', 'doorsturen' en zelfs 'ontvangen', inzien en 'verwijderen' vallen daaronder. Zo bezien zou je wellicht toch ook nog eens bij het ledenbestand van de tennisvereniging stil moeten staan.

3.1 Overwegingen bij de verwerking van persoonsgegevens

3.1.1 Een legitieme basis voor de verwerking

Iedere verwerking van persoonsgegevens is gebonden aan (sectorspecifieke) wet- en regelgeving. De vaststelling welke wet- en regelgeving van toepassing is voor een specifieke organisatie en/of activiteiten is reeds beleidsmatig bepaald op organisatieniveau (B.02/02). Hierbij wordt op bedrijfsniveau bepaald of de organisatie is ingericht voor de verwerking van persoonsgegevens.

Twee analyses bepalen de keuze voor de verwerking van persoonsgegevens:

1. **De vraag naar de rechtmatigheid:**
   Maak met behulp van criterium U.01 een analyse die uitwijst of het doel van de verwerking een rechtmatige grond kent. Past het doel van ieder te verwerken persoonsgegeven binnen de op organisatieniveau bepaalde rechtmatige gronden? Zo ja, dan kan daaraan gerefereerd worden. Past het niet binnen de bestaande gronden, dan moet de vraag gesteld worden of de organisatie legitiem de gewenste gegevens kan verwerken. Dit kan leiden tot de vervolgvraag of bijstelling van de bedrijfsdoelstelling mogelijk en verdedigbaar is naar de betrokkene(n) en de toezichthouders. Zo niet, dan bestaat er geen legitimering voor het verwerken van de persoonsgegevens, zoals vereist in criterium C.01.

2. **De vraag naar de noodzaak:**
   Het omschreven doel biedt een kader waaraan getoetst kan worden of de verwerking van de gegevens noodzakelijk is voor het bereiken van het doel (U.01). Bij ieder voornemen om een persoonsgegeven te gaan verwerken moet (door het raadplegen van het register van verwerkingsactiviteiten (U.02)) bepaald worden of het gegeven al verwerkt wordt binnen de eigen organisatie, dan wel of het gegeven al door een ketenpartij wordt verwerkt. Indien het gevraagde gegeven reeds elders voorhanden is kun je de keuze maken het gegeven daar te laten en daar de bedrijfslogica onder te brengen, in plaats van de verwerking in eigen huis te nemen[11].

Is de verwerking rechtmatig en noodzakelijk dan wordt de verwerking van de persoonsgegevens vastgelegd en opgenomen in het register van verwerkingsactiviteiten (U.02). Deze registratieplicht geldt niet bij een kleine organisaties, waarbij er weinig risico's voor de rechten en vrijheden van de betrokkenen zijn (zie U.02/01.06).

Het verwerken van persoonsgegevens start met het vaststellen van de rechtmatigheid én de noodzaak.

[11] Een voorbeeld hiervan is het centraal registeren van medicijngebruik, waarbij de controle of een nieuw medicijn risico oplevert voor de patiënt niet gebeurt door het opvragen van de gegevens, maar dit door aan de centrale registratie te laten doen.

3.1.2 De omvang van de verzameling

Voor iedere verzameling (en dus: verwerking) van persoonsgegevens geldt het vereiste dat deze toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking, ook wel dataminimalisatie genoemd) (U.01/02.01). Dit betekent dat alleen die persoonsgegevens mogen worden uitgevraagd die nodig zijn om het doel te bereiken, waarbij de verzamelde persoonsgegeven aantoonbaar in relatie staan tot het doel en dat het doel niet met minder gegevens kan worden bereikt. Onnodige uitvraging kan worden voorkomen door bij de analyse van de rechtmatigheid en noodzaak (paragraaf 3.1.1) ook te kijken naar de voor de verwerking te verzamelen gegevens. Deze analyse en een besluit of beslissing op basis daarvan moeten gedaan zijn vóór de uitvraging van een persoonsgegeven effectief plaatsvindt en moeten, inclusief de afweging, worden vastgelegd voor het informeren van de betrokkene(n) en eventuele verantwoording aan de toezichthouder (U.02). Door deze afweging (ook) vast te leggen in het register (zie hoofdstuk 5) kan deze eenvoudig meegenomen worden in het overzicht van verwerkte persoonsgegevens. Zo is de afweging beschikbaar voor controledoeleinden (criteria C.01 en C.02) en kan onnodige uitvraag worden voorkomen. Een voorbeeld in dit kader is federatief authenticatiebeheer.

Voorbeeld: Het beperken van de omvang door federatief authenticatiebeheer.
Een vorm van authenticatie is vereist voor iedere dienst die persoonsgegevens verzamelt of toont. Dit vraagt om het verzamelen en bijhouden van identificatie- en authenticatiegegevens. Dit zijn dus óók persoonsgegevens.
De inzet van federatieve authenticatie bij een andere partij kan de omvang van de eigen verzameling van persoonsgegevens beperken. Deze andere organisatie of Trusted Third Party (TTP) beschermt de identificatie- en authenticatiegegevens voor alle aangesloten organisaties, die daarmee dus allemaal de omvang beperken.

Van ieder verzameld persoonsgegeven is aangetoond
dat deze toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is
voor de doeleinden waarvoor zij worden verwerkt
(“dataminimalisatie”).

3.1.3 Een GEB voor 'iedere verdere verwerking'?

Als je persoonsgegevens gaat verwerken, dan is een GEB verplicht (B.03). Dit geldt voor alle verwerkingen, ook voor iedere 'verdere verwerking'. Juist bij verdere verwerkingen is het niet altijd evident dat dit gebeurt[12]. Het “verder verwerkingen” sluipt gemakkelijk ongemerkt in de processen (door bijvoorbeeld onoplettendheid bij noodzakelijke of gewenste procesveranderingen), *nadat* de verplichte oorspronkelijke GRB heeft plaatsgevonden. Een voorbeeld is het gebruiken van persoonsgegevens bij het uitprinten van een nieuwe brief of in een werkblad. Ook deze verdere verwerking is gebonden aan de privacyvereisten en daarmee dus GEB-plichtig.

Het waarborgen van de privacy bij een verdere verwerking is situationeel en vraagt om een situationele aanpak, waarbij de wijze van in control zijn en de belangen van de betrokkene met elkaar in evenwicht zijn.

Met de onderstaande analyse en aanpak is het mogelijk dat organisaties aantoonbaar de privacy waarborgen zonder blokkades voor de bedrijfsvoering of het dienen van de (privacy)belangen van de betrokkene. Stel bij iedere aanpassing van de verwerking vast in welk kwadrant de aanpassing past:

[12] Een ''verdere verwerking'' betreft in de regel een verwerking van een persoonsgegeven met een doel dat buiten de oorspronkelijke scope van een verwerkingsproces valt. Daarbij kan het ook gaan om een aanpassing aan het oorspronkelijke proces, bijvoorbeeld vanwege gewijzigde omstandigheden of behoeften.

Aard van de verwerking	conform of verenigbaar met oorspronkelijk doel	niet conform of verenigbaar met oorspronkelijk doel
structureel	De verdere verwerking vindt buiten de oorspronkelijke geplande verwerking plaats, maar is *structureel* onderdeel (geworden) van het oorspronkelijke werkproces en is *conform* het oorspronkelijke doel geminimaliseerd (U.01).	De verdere verwerking vindt buiten de oorspronkelijke geplande verwerking plaats en is *structureel*, maar heeft een afwijkend doel en vindt daarmee *niet conform* criterium U.01 van het oorspronkelijke werkproces plaats (niet geminimaliseerd).
incidenteel	De verdere verwerking vindt buiten de oorspronkelijke geplande verwerking plaats en is *incidenteel*, maar gebeurt *conform* criterium U.01 van het oorspronkelijke werkproces: geminimaliseerd.	De verdere verwerking vindt buiten de oorspronkelijke geplande verwerking plaats maar is *incidenteel* en heeft een afwijkend doel; vindt dus *niet conform* criterium U.01 van het oorspronkelijke werkproces plaats (niet geminimaliseerd).

Hieronder staat in overeenkomstige kwadranten wat het in pragmatische termen betekent voor de organisatie:

Keuze voor een GEB	conform of verenigbaar met oorspronkelijk doel	conform of verenigbaar met oorspronkelijk doel
structureel	Deze uitbreiding vormt geen eigen verwerking en vraagt dus niet om een eigen GEB. Indien deze uitbreiding op het proces nog niet is meegenomen in de GEB van dat werkproces c.q. de verwerking, dan kan de uitbreiding eenvoudig toegevoegd worden in de GEB op dat werkproces.	Deze uitbreiding vormt een eigen verwerking, omdat het een ander doel betreft dan de oorspronkelijke verwerking, waarvoor een GEB is uitgevoerd. Doordat deze uitbreiding structureel van aard is, is een GEB mogelijk en in dit geval dus een aparte, eigen GEB.
incidenteel	Door het incidentele karakter van deze verdere verwerking is het moeilijk of soms zelfs onmogelijk met enige trefzekerheid een GEB uit te voeren. Wel moet de individuele bewerker minimaal bepalen of aan de criteria U.03 t/m U.04 wordt voldaan. Ook moet controle nog mogelijk zijn door te voldoen aan de criteria C.01 en C.02. Om te voorkomen dat voor de controle op de verdere verwerking een eigen registratie moet worden aangelegd, kan de gehanteerde logica en de resultaten in het oorspronkelijk systeem worden vastgelegd. Wanneer de individuele bewerker niet aan de criteria kan voldoen, bv door het ontbreken van een afdoende informatiebeveiliging, dan moet de bewerker afzien van de verdere verwerking.	De incidentele verdere verwerking vormt altijd een eigen verwerking, omdat zij een ander doel heeft dan de oorspronkelijke verwerking waarvoor een GEB is uitgevoerd. Door het incidentele karakter ervan verdere verwerking is het moeilijk of soms zelfs onmogelijk om trefzeker een GEB uit te voeren. Belangrijk verschil met hiernaast is dat er geen legitimering conform het doel van de oorspronkelijke verwerking is. Legitimering is door het incidentele karakter alleen mogelijk door aan te tonen dat het belang van de betrokkene wordt gediend en dit vast te leggen. Deze legitimering is vereist en kan het best worden bewerkstelligd door de verdere verwerking en het belang ervan met de betrokkene af te stemmen en vast te leggen, en dit voorafgaand te doen aan het gebruik van de resultaten van deze verdere verwerking. Daarnaast moet de individuele bewerker ook hier minimaal bepalen of aan de criteria U.03 t/m U.04 wordt voldaan. Ook moet controle nog mogelijk zijn door te voldoen aan de criteria C.01 en C.02. Om te voorkomen dat voor de controle op de verdere verwerking een eigen registratie moet worden aangelegd, kunnen de gehanteerde logica en de resultaten in het oorspronkelijk systeem worden vastgelegd. Wanneer de individuele bewerker niet aan de criteria kan voldoen, bijvoorbeeld door het ontbreken van een afdoende informatiebeveiliging, dan moet de bewerker afzien van de verdere verwerking.

4 De inrichting van de verwerking

Betrokkenen hebben het recht te weten waarvoor hun persoonsgegevens worden gebruikt, op welke wijze en door wie. De organisatie heeft hiertoe een informatieplicht (U.05) bij de verzameling van de gegevens en wanneer de betrokkene daarom vraagt (C.02). Om hieraan tegemoet te kunnen komen is vereist vooraf zorgvuldig nadenken over de inrichting van de verwerking.

4.1 Transparantie naar de betrokkene

4.1.1 Informeren van de betrokkene over de verwerking

Ontvangst van persoonsgegevens (de Avg spreekt van 'verzameling') is niet toegestaan als de betrokkene niet tijdig wordt geïnformeerd, tenzij een uitzonderingsgrond voor deze informatieverplichting geldt (zie hiervoor criterium U.05).
Op verschillende manieren kunnen bij een gegevensverwerking gegevens worden verzameld:

1. Ontvangst direct van de betrokkene;
2. Ontvangst vanuit de eigen gegevensvastlegging binnen de eigen organisatie;
3. Vastlegging van een waarneming door de eigen organisatie zelf;
4. Ontvangst van een ketenpartij.

Voor de verschillende manieren van ontvangst gelden specifieke aandachtspunten:

Ad 1: Bij ontvangst direct van de betrokkene wordt de betrokkene tijdig geïnformeerd over het doel van de verwerking etc. Onder tijdig wordt verstaan: voorafgaand aan de ontvangst van de persoonsgegevens.

Ad 2-4: De keuze om gegevens afkomstig van andere gegevensverwerkingen te verwerken vraagt om een vaststelling van de verenigbaarheid met de oorspronkelijke gerechtvaardigde doelen (U.01/03 t/m U.01/08). Ook moet helder zijn of de betrokkene op de hoogte is van deze verzameling van de persoonsgegevens (U.05).
Is de betrokkene nog niet op de hoogte van de (nieuwe) gegevensverwerking, bijvoorbeeld doordat er geen verenigbaarheid is met de oorspronkelijke gerechtvaardigde doelen, dan moet de betrokkene worden geïnformeerd over de beslissing om de eerder voor een ander doel verzamelde gegevens te verwerken voor het betreffende (nieuwe) doel.
Is er een uitzondering en is deze formeel vastgesteld (conform U.05/04), dan geldt deze plicht niet. Wel moet vastgelegd worden welke uitzonderingsregel het betreft.
Informatie over de niet van betrokkene verkregen persoonsgegevens wordt binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens[13].

Over iedere verzameling moet de betrokkene geïnformeerd worden, tenzij daarvoor een uitzondering geldt (U.05.04). Indien de betrokkene geïnformeerd moet worden, moet de betrokkene in ieder geval geïnformeerd worden over de identiteit van de verantwoordelijke en de doelen van de gegevensverwerking(en). Hoe daarbij de privacy gewaarborgd wordt moet in voor de betrokkene begrijpelijke tekst worden uitgelegd. De inhoudsvereisten staan beschreven in de Privacy Baseline (U.05/02).

4.1.2 Ontsluiten van verwerkte persoonsgegevens voor betrokkenen

Betrokkenen hebben recht op inzicht van de persoonsgegevens, zoals die ten behoeve van de gegevens-verwerking in de organisatie zijn vastgelegd en worden bewaard. Het is daarom van belang de presentatie van persoonsgegevens aan betrokkenen mee te nemen bij ontwerp en bouw van de gegevensverwerking.
Bedenk daarbij dat de informatiebehoefte van de bewerkers en de betrokkenen niet noodzakelijkerwijs 1 op 1 overeenkomen. Dat kan ook gelden voor de presentatiewijze van de gegevens. Om die reden moet inzage door betrokkenen worden geregeld in een service die de ontsluiting van de persoonsgegevens of dossiervoorziening op maat aanbiedt naar de (redelijke) behoefte van betrokkenen.

[13] Art. 14 lid 3 Avg of U.05/01.02 Privacy Baseline

Het effectief bieden van transparantie aan betrokkenen vraagt om een passende ontsluitingsvoorziening.

Deze voorziening moet de gegevens zo presenteren dat de betrokkene een voldoende volledig overzicht krijgt om de rechtmatigheid te kunnen bepalen (C.02). Daarnaast is het ook van belang dat de betrokkene de kwaliteit (juistheid) van de gegevens kan controleren en bij onjuistheid kan (laten) aanpassen (U.03). Deze mogelijkheid komt terug in paragraaf 6.2.

De ontsluiting van de gewenste persoonsgegevens verhoudt zich zelden lineair en 1 op 1 tot de structuur van applicaties en/of de (daarbinnen) vastgelegde gegevens. Het bieden van transparantie wordt daardoor moeilijker, zeker als de gegevensverwerking geschiedt in een palet aan applicaties. Het advies is daarom het volgende principe te hanteren:

Per doel en bij voorkeur voor meerdere doelen voor gegevenswerkingen wordt maximaal één voorziening / applicatie gehanteerd.

4.2 Transparantie borgen in het ontwerp

4.2.1 Transparantie door een geordende gegevensverwerking

Door binnen de bedrijfsprocessen de persoonsgegevens zoveel mogelijk geautomatiseerd te verwerken volgens formeel bepaalde logica, bijvoorbeeld in een Business Rule Managementsysteem (BRM) en handmatige acties geautomatiseerd toe te kennen medewerkers, bijvoorbeeld via een Workflow Management (WFM) systeem, kan de doelbinding van een verwerking binnen de processen relatief eenvoudig worden aangetoond. Hier is immers sprake van repeterende procespatronen, waarbij activiteiten in voldoende mate van detail formeel gespecificeerd zijn. Met de specificatie van iedere activiteit kan ook het doel van iedere activiteit formeel worden vastgelegd.

Het geautomatiseerd uitwisselen van gegevens tussen bedrijfsprocessen en het geautomatiseerd toekennen van taken die handmatige acties vragen vereenvoudigen het aantonen van doelbinding.

Het geautomatiseerd toekennen van handmatige acties vraagt om een standaard werkwijze binnen de bedrijfsprocessen. Handmatige acties zijn in dit verband de door bewerkers uitgevoerde verwerkingen als verlengstuk op de geautomatiseerde verwerking.
Wanneer het werkproces niet in een vast protocol vastligt, maar afhankelijk is van kennis van bewerkers en hun kennis van regelgeving, dan is het van belang dat wordt vastgelegd (gelogd) wat deze werkers doen met de persoonsgegevens in de verwerking. Het gebruik van specifieke persoonsgegevens is situationeel, maar moet steeds aantoonbaar passen binnen de doelbinding. Dit kunnen aantonen is alleen mogelijk door middel van continue logging, bijvoorbeeld in een Document Management Systeem (DMS) dat het gebruik vastlegt.

Indien binnen een bedrijfsproces het gebruik van persoonsgegevens situationeel is, vraagt het kunnen aantonen van de doelbinding om logging van het gebruik.

4.2.2 Transparantie door een geautomatiseerde gegevensverwerking.

Bij de handmatige verwerking van persoonsgegevens krijgen bewerkers toegang tot de persoonsgegevens. In het ontwerp kan door middel van een volledig geautomatiseerde verwerking, ofwel 'straight through processing' worden voorkomen dat meerdere bewerkers toegang moeten krijgen tot de persoonsgegevens. Daarbij biedt straight through processing het voordeel dat altijd volgens dezelfde formeel vastgelegde bedrijfslogica en met een eenduidige kwaliteit wordt verwerkt.

'Straight through processing' voorkomt onnodige toegang van bewerkers tot persoonsgegevens.

4.3 Privacy borgen met een passende granulariteit

Voor de verschillende verwerkingen van de gegevens van een betrokkene is het niet altijd nodig dat de betreffende bewerker toegang heeft tot de hele 'bundel' van de persoonsgegevens van een betrokkene. Om ervoor te zorgen dat niet onnodig vertrouwelijke gegevens aan verwerkers getoond worden is granulariteit nodig waarmee toegang tot 'alles of niets' kan worden verfijnd. Evidente voorbeelden zijn een onderscheid tussen NAW- en bijzondere of gevoelige gegevens, maar ook binnen de (deel) rubrieken kan onderscheid heel zinvol zijn. Scheiden van gegevens is mogelijk door gegevens en functies die samenhangen in het systeem, inclusief services in een Service Oriented Architectuur, op een juiste manier te clusteren. Dit doe je door gegevens en functionaliteit die een bepaalde vertrouwelijkheid kennen te onderscheiden van gegevens die niet tot hetzelfde doel (U.01) behoren. Dit maakt het mogelijk een procesbesturing, verwerking en datamodel te hanteren waarbij eenvoudig services kunnen worden ontworpen met de gewenste granulariteit[14].

De hier gebruikte definitie voor granulariteit is: *Granulariteit is de mate van detaillering.* Bij een beperkte mate van granulariteit is sprake van een beperkte differentiatie. Een beperkte differentiatie leidt mogelijk tot onnodige toegang tot gegevens.
Bij het ontwerp van een systeem wordt het implementeren van de juiste granulariteit ondersteund door het hanteren van een meerlagen technische architectuur[15]. Door het bewust hanteren van een meerlagen architectuur kan bij het ontwerp bewust de granulariteit binnen iedere laag gekozen worden. De volgende proceslagen worden voor de uitleg gehanteerd:

1. **Procesbesturingslaag:** Deze laag beschrijft een geordende reeks van processtappen die in z'n geheel bij één verantwoordelijke of organisatorische eenheid belegd kan worden om een specifieke bijdrage te leveren bij de verwerking van de persoonsgegevens. Een processtap is hierbij een reeks handelingen die ononderbroken wordt uitgevoerd door één mens of machine.
2. **Verwerkingslaag:** In de verwerkingslaag is de functionaliteit van een applicatie ondergebracht. De functionaliteit bestaat bijvoorbeeld uit verwerkingslogica met daarin de businesslogica.
3. **Gegevenslaag**: In een gegevenslaag zijn die gegevens ondergebracht die bewerkt worden door de verwerkingslaag.

Het bewust hanteren van deze drie lagen helpt overigens ook bij het effectief inrichten van autorisaties of is daarvoor zelfs randvoorwaardelijk.

4.3.1 Granulariteit in de gegevenslaag

Door gegevens in de gegevenslaag gescheiden van elkaar op te slaan en af te schermen is een fijnmazige granulariteit mogelijk. Bij opslag in ongestructureerde bestanden daarentegen zijn door het ontbreken van een structuur de gegevens niet separaat af te schermen.
Bij het opzetten van de gegevensopslag wordt de structuur het beste geboden door het hanteren van een datamodel. Als er geen datamodel wordt gehanteerd vindt afscherming en opvraging per gegeven plaats. Dit leidt tot een fijnmazige functionaliteit en tot een hoge beheerlast van fijnmazige autorisaties.
Wordt een datamodel gehanteerd, dan kunnen gegevens afgeschermd en opgevraagd worden per gegevensgroep. Een gegevensgroep is een verzameling van gegevens die in functionele zin en qua doelbinding een sterke samenhang vertonen. Door de granulariteit te baseren op dergelijke gegevensgroepen is de toegang beheersbaar te maken en te houden.

Hanteer bij de opslag van gegevens een datamodel. Hanteer binnen het datamodel een granulariteit op basis van gegevensgroepen, waarbinnen de gegevens in functionele zin en qua doelbinding een sterke samenhang vertonen.

[14] Tip: het scheiden van gegevens maakt ook het (op maat) vernietigen van gegevens eenvoudiger.
[15] Er bestaat een veelheid aan architectuurmodellen. Zonder daaraan afbreuk te doen beperken we ons in dit document tot een architectuurmodel met daarin 3 lagen: procesbesturingslaag, verwerkingslaag en gegevenslaag. Met dit model kan goed aangegeven worden hoe de privacy door middel van granulariteit in gegevensverzamelingen en functies kan worden gewaarborgd.

4.3.2 Granulariteit in de verwerkingslaag

Het niet juist bepalen van de gewenste granulariteit van functies en services in de verwerkingslaag beïnvloedt de beheerbaarheid en de performance van de verwerking nadelig. Een onjuiste granulariteit beïnvloedt echter ook de privacy.

1. **Beheer vs. privacy:**
   Beheer van functies en services is eenvoudiger door te kiezen voor een grove(re) granulariteit. Minder verschillende functies en services vraagt simpelweg minder beheer. Grove(re) granulariteit betekent echter ook dat een functie of service een uitgebreide gegevensset toont. Als deze gegevensset meer persoonsgegevens toont dan nodig voor het doel waarvoor de gegevens worden opgevraagd komt daarmee de privacy in gevaar.
2. **Performance vs. privacy:**
   Een grove granulariteit beperkt het aantal aanroepen naar functies en services. Dit leidt doorgaans tot een betere performance. Ook hier leidt een grove granulariteit, wanneer teveel persoonsgegevens worden getoond, weer tot het in gevaar brengen van de privacy.

Bij de keuze van de granulariteit van de functies en services is het van belang te kijken naar de samenhang tussen de gegevens. Een gegevensgroep is een set van gegevens die een logisch geheel vormen. Een gegevensgroep "locatie" bestaat bijvoorbeeld uit de combinatie van straatnaam, huisnummer en woonplaats. Door de granulariteit van de functies en services, bij voorkeur één op één, te mappen op gegevensgroepen wordt de juiste balans gevonden tussen de beheerbaarheid, flexibiliteit, performance en privacybescherming.

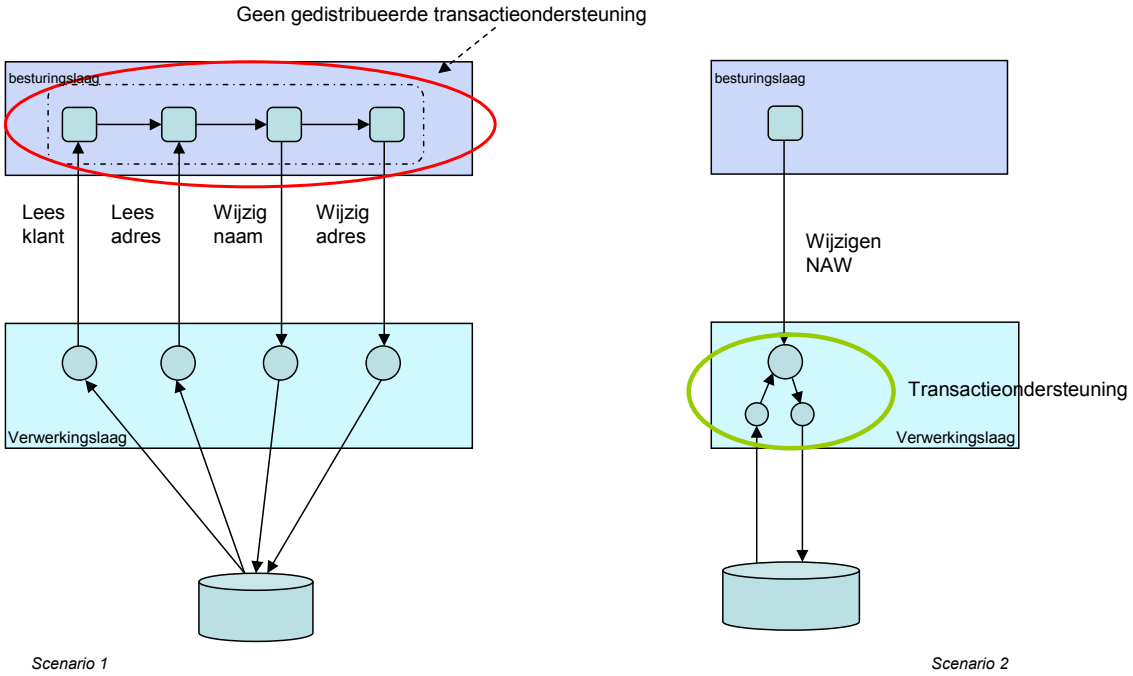
Hanteer een granulariteit waarbij de afscherming van functies en services aansluit op die van gegevensgroepen, zodat alleen persoonsgegevens worden meegestuurd die passen binnen het doel van de beoogde functie of service.

4.3.3 Granulariteit in de procesbesturingslaag

De procesbesturingslaag knipt een proces gestructureerd op in processtappen. Bij het opknippen van het proces moet er aandacht zijn voor de granulariteit van de processtappen. Modellen met een grofmazige granulariteit zijn overzichtelijk, omdat zij uit een beperkt aantal stappen bestaan. Modellen met een fijnmazige granulariteit zijn meer gedetailleerd en daardoor wellicht moeilijker te doorgronden.
Het advies is voor de granulariteit van de processtappen als regel te hanteren dat wijzigingen binnen één gegevensgroep in één processtap wordt uitgevoerd.

Hanteer een fijnmazige granulariteit waarbij processtappen en handelingen toegewezen kunnen worden aan één persoon, zonder dat een te fijnmazige granulariteit leidt tot inconsistenties in de gegevensverzamelingen of tot overhead om inconsistentie te voorkomen.

Inconsistenties in de gegevensverzamelingen kunnen optreden door het slechts deels uitvoeren van gerelateerde processtappen of handelingen. Het gebruik van fijnmazige processtappen leidt tot transacties, waarbij bewaking van de gerelateerde transacties nodig is (scenario 1 in onderstaande figuur).



Figuur: Fijnmazig processtappen vs. grofmazige processtappen.

5 Gegevensmanagement

5.1 Metagegevens

Bij gegevens kan onderscheid worden gemaakt tussen gestructureerde gegevens en ongestructureerde gegevens. Door gegevens te voorzien van metagegevens wordt een betekenis ("uitleg") aan de gegevens gegeven, wordt de vindbaarheid vergroot en is het eenvoudiger bij te houden welke gegevens waarvoor (mogen) worden gebruikt. Door het meegeven van de betekenis wordt de kans op onjuist gebruik van de gegevens door *multirealiteit* verminderd. Het onderkennen van multirealiteit en het vastleggen ervan in de metagegevens is een belangrijk onderdeel van kwaliteitsmanagement (U.03)[16].
Door het vastleggen van de metagegevens wordt gegevensmanagement met het register (U.02) eenvoudiger mogelijk. Door bij de gegevens in de metagegevens tevens het doel van de gegevens vast te leggen is bewaking van de doelbinding (U.01) beter mogelijk.

Metagegevens zijn ondersteunend bij gegevensmanagement, kwaliteitsmanagement en het bewaken van de doelbinding.

Het *aantoonbaar* onder controle hebben van privacy is alleen mogelijk als bekend is welke persoonsgegevens worden verzameld, verwerkt en bewaard en met welk doel. Dit is in de grond van de zaak een administratief proces van het bijhouden van gegevens. Gegevensmanagement gaat echter verder dan alleen het bijhouden. Door bij het ontwerp van de systemen actief gebruik te maken van de administratie kan hergebruik van gegevens worden mogelijk gemaakt en wordt gekeken of de gegevens toereikend, ter zake dienend en niet bovenmatig zijn. Belangrijk hierbij is de juistheid van de administratie. Bij gestructureerde gegevens, zoals die bijvoorbeeld voorkomen in databases en XML bestanden, kunnen de gegevens voorzien worden van zogenaamde tags (verder uitgelegd in paragraaf 5.2). Ongestructureerde gegevens kunnen door middel van fileanalyse worden onderzocht op de aanwezigheid van persoonsgegevens (verder uitgelegd in paragraaf 5.3).

5.2 Tags

Een tag is een label dat metagegevens bevat. Een tag bevat dus 'informatie over informatie' en is daarmee een label dat informatie geeft over de inhoud van een bestand of gegevensveld. Tags kunnen op verschillende manieren worden toegepast. Ze kunnen door de gebruiker - of in de applicatie door de gegevensbeheerder - worden gevuld met informatie.
Tags kunnen door gebruikers gebruikt worden voor het gemakkelijker kunnen vinden van bestanden; voor het beheer van gegevens (gegevensmanagement) zijn tags nuttig voor het verbeteren de privacy, doordat beter wordt bijgehouden wat een gegeven inhoudt en dus of het bijvoorbeeld verouderd is of een andere betekenis heeft en daardoor zou kunnen leiden tot verkeerde conclusies.

Een voorbeeld: VIP''s, zoals bekende Nederlanders of personen die extra bescherming nodig hebben, staan in de belangstelling van velen, die niet zelden ook op jacht gaan naar gegevens. Door bijzondere gegevens of gegevens over VIP''s, in een tag als zodanig te markeren, kan de toegang tot deze gegevens onderworpen worden aan een extra controle op verdacht of onrechtmatig gebruik van toegangsrechten.

[16] Over het algemeen spreekt men van administratieve multirealiteit wanneer verschillende definities van een gelijknamig gegeven bestaan binnen een organisatie. Zo omvat bij UWV het gegeven "arbeidsverleden" in de context van de WW-berekening heel andere informatie (te weten: contractuele dienstverbanden) dan in de context van bemiddelingsondersteuning, waar het meer 'werkervaring in het algemeen' bedoelt weer te geven. Deze verschillen zijn functioneel en nodig, soms zelfs ook voor privacydoeleinden, maar maken wel een precies gegevensmanagement noodzakelijk.

De categorieën van bijzondere persoonsgegevens kunnen door ze in een tag als zodanig te markeren gericht onderworpen worden aan een extra controle op verdachte of onrechtmatige toegang.

Bedenk wel dat doordat in tags informatie over gebruikers opgeslagen kan worden tags ook privacyrisico's kunnen opleveren. Tools voor tagmanagement maken het beheer van de tags beter mogelijk en kunnen daardoor weer bijdragen aan de privacy.

5.3 Fileanalyse

Tools voor fileanalyse analyseren, indexeren, zoeken, volgen en rapporteren over metadata en, in sommige gevallen, de inhoud van bestanden. De resultaten kunnen vervolgens gebruikt worden om de privacy te waarborgen, bijvoorbeeld doordat ze gebruikt kunnen worden om aan te geven wat de levensduur van de informatie is en daarmee de (on)geldigheid ervan. Verouderde vertrouwelijke informatie kan zo tijdig worden vernietigd. Onnodig te zeggen dat ook het gehoor geven aan het 'recht vergeten te worden' op deze wijze ingeregeld kan worden.

Het gebruik van metadata is in het bijzonder noodzakelijk wanneer oude informatie nog is opgeslagen in beeld- en geluidsbestanden die geen bewerkbare tekst bevatten en daardoor slechts via een zoekmachine gevonden kunnen worden als toevallig de titel het gezochte trefwoord bevat. Ook gecomprimeerde (gezipte) tekstbestanden zijn niet altijd te doorzoeken, en versleutelde (met wachtwoord beschermde) documenten al helemaal niet. Tagging biedt dan de mogelijkheid om toch trefwoorden of categorie-aanduidingen aan bestanden toe te kennen, zodat ze gevonden kunnen worden zonder de inhoud te hoeven kennen.

Tools voor fileanalyse bij voorkeur samen met het gebruik van tags met metadata geven de mogelijkheid de privacy-vereisten in te vullen

6 Kwaliteitsmanagement

Kwaliteitsmanagement zorgt voor de processen die de juistheid en nauwkeurigheid van de persoonsgegevens bewaken en die, bij onjuistheid en onnauwkeurigheid van de gegevens, de gegevens corrigeren. Verkeerde conclusies over de betrokkene kunnen getrokken worden met negatieve consequenties voor de betrokkene, wanneer:

1. De gegevens onjuist en onnauwkeurig zijn ingevoerd of gecorrumpeerd zijn geraakt;
2. De gebruikte logica (de gebruikte redenatie) onjuist is.

Het voorkomen van onjuistheden is in het belang van zowel de betrokkene als de bewerker. Beiden dienen in staat te zijn de onjuistheid en onnauwkeurigheid van de gegevens te voorkomen, te constateren en zo nodig te corrigeren.

6.1 Het voorkomen van onjuiste of onnauwkeurige gegevens

Onjuiste gegevens kunnen ontstaan door het opslaan van strijdige gegevens of door het doorvoeren van incomplete transacties in gegevensverzamelingen. Dit kan voorkomen worden door:

1. **Controle en correctie door betrokkene**
   De betrokkene heeft de mogelijkheid om een controle op de juistheid van de gegevens uit te (laten) voeren en deze desgewenst kunnen (laten) corrigeren. Dit bij voorkeur vóórdat de gegevens worden verwerkt.
2. **Interne controle**
   Interne controle betekent het inbouwen van kwaliteitscontroles die aangeven of een gegeven strijdig is met andere gegevensbronnen. Het belang van interne controle gaat echter verder dan dat. Het gebruik van de juiste logica, bijvoorbeeld bij profiling, om tot nieuwe en juiste conclusies te komen moet mee-genomen worden bij de interne controle. Deze interne controle begint al bij het ontwerp van de systemen en maakt daarmee wezenlijk onderdeel uit van Privacy by Design.
3. **Transactie-integriteit**
   Bij een transactie worden gegevens gewijzigd. Door transactiemanagement kun je borgen dat deze wijzigingen in samenhang worden uitgevoerd, en ofwel allemaal plaatsvinden, ofwel geen van alle, zodat de gegevens tijdens de transactie niet onbedoeld veranderen.

Het verbeteren van de gegevensverwerking zal in vele gevallen leiden tot een toename in complexiteit die eerder leidt tot extra fouten (cascade effecten), dan tot een verbetering. Het is belangrijk hier bij het ontwerp van de systemen rekening mee te houden en van meet af aan de complexiteit van gegevensverwerkingen beperkt te houden. Binnen het architectuurdomein wordt de complexiteit van een systeem aangeduid met het aantal terugkoppelingen (lussen) die zich in de procesflow van de gegevensverwerking bevinden.

Streef bij het ontwerpen naar een lineaire verwerking van gegevens, door het aantal terugkoppelingen te beperken, zodat helder blijft wat de gevolgen zijn van de verwerking.

Indien administraties of opslagmedia worden gebruikt die niet te wijzigen zijn, zorg er dan voor dat informatie over de juistheid en nauwkeurigheid van de gegevens wordt opgenomen in de gegevensverwerking. Dit kan door het toevoegen van een "kwaliteitsindicatie" bij het gegeven, die in de verwerking kan worden meegenomen. Dit kan een extra informatieveld zijn in de gegevensopslag. De kwaliteitsindicatie kan vervolgens worden meegenomen in de gegevensverwerking en daarmee de output van de gegevensverwerking, zoals een besluit voor een betrokkene, beïnvloeden.

6.2 Controle en correctie door betrokkene

Een betrokkene moet inzage hebben in de gegevens en de verwerkingen die op zijn of haar persoon betrekking hebben. Bij gebleken onjuistheid van de gegevens of onrechtmatigheid van de verwerking kan de betrokkene eisen dat de fouten worden gecorrigeerd dan wel de verwerking wordt gestopt.

6.2.1 Inzagerecht

Inzagerecht is een eerste vereiste om de betrokkene de mogelijkheid te geven om zijn rechten uit te oefenen. De vraag daarbij is of de inzage de betrokkene daarvoor voldoende inzicht geeft. Om op een efficiënte en passende wijze transparantie te kunnen bieden aan de betrokkene is het allereerst vereist zelf voldoende inzicht in de eigen organisatie te hebben, zodat de betrokkene bediend kan worden met zinvolle, relevante informatie en om desgewenst meer in detail in te kunnen zoomen op een specifieke verwerking.

Transparantie voor betrokkenen start met transparantie in de eigen organisatie. Transparantie vraagt om een view die is afgestemd op de doelgroep.

De mogelijkheid voor betrokkenen om inzage te hebben, de gegevens te corrigeren of te verwijderen kan worden ondersteund door een logboek voor gegevenstransacties, waarin wordt bijgehouden welke persoonsgegevens aan een organisatie (bewust of onbewust) zijn doorgegeven. Een dergelijk logboek vergroot niet alleen het inzicht voor de betrokkene. Het helpt ook de interne organisatie inzicht te krijgen en te houden op datastromen, verstrekkingen en de doelen waarvoor gegevens zijn verstrekt. Dit voorkomt verwerkingen, inclusief profiling, van persoonsgegevens die daar niet voor bedoeld zijn.

Een logboek voor gegevenstransacties vergroot het inzicht voor betrokkene én bewerker over welke gegevens waarvoor zijn ontvangen en gebruikt.

6.2.2 Correctierecht voor betrokkene

De betrokkene heeft het recht om persoonsgegevens te laten corrigeren als de betrokkene van mening is dat die onjuist zijn. De Baseline geeft aan aan welke eisen de correctiemogelijkheden moeten voldoen. De binnen de Avg vereist correctiemogelijkheden, maken het mogelijk de juistheid en nauwkeurigheid van persoonsgegevens te bewaken en desgewenst de verwerking te laten staken of de persoonsgegevens te (laten) corrigeren of overgedragen te krijgen.
Belangrijk is dat de betrokkene daadwerkelijk wordt beschermt en voorkomt dat de betrokkene in de problemen komt. Dit gaat verder dan alleen het wijzigen van de foutieve persoonsgegevens. Kennis van mogelijke gevolgschade is daarbij evenzeer van belang. Dat betekent dat verwerkingen en transacties van elk gegeven moeten kunnen worden nagezien. Vervolgbewerkers of ontvangers moeten eveneens op de hoogte worden gesteld van de foutieve persoonsgegevens en deze corrigeren of verwijderen. Wellicht is het niet mogelijk voor alle verzoeken op een geautomatiseerde wijze te repareren en schade te voorkomen. Hou er rekening mee dat een deel van de correctieverzoeken zullen blijven leiden tot maatwerk (handwerk) voor de specifieke betrokkene en het bieden van ondersteuning om de gevolgen voor hem of haar te beperken.

Het correctierecht gaat verder dan het corrigeren van de foutieve gegevens. Voor de betrokkene moet voorkomen worden dat hij of zij nadelige gevolgen ondervindt.

6.3 Interne controle

Het inbouwen van kwaliteitscontroles die controleren of een gegeven strijdig is met andere gegevensbronnen voorkomt het gebruik van strijdige gegevens en de noodzaak gegevens (met terugwerkende kracht) in een latere fase te moeten corrigeren. Het in een latere fase corrigeren van de gegevens leidt, omdat dit bij de bron van de gegevens moet gebeuren, mogelijk tot complexe terugkoppelingen. Daarmee zijn deze strijdig met het streven naar lineaire verwerking van persoonsgegevens (zie paragraaf 6.1), waardoor mogelijk niet meer helder is wat de gevolgen zijn van het wijzigen van de persoonsgegevens.

Kwaliteitscontroles voorafgaand aan de verwerking voorkomen complexe correcties achteraf.

6.4 Transactie-integriteit

De integriteit van gegevens - letterlijk: de "ongeschondenheid" - gaat over de juistheid (integrity) van opgeslagen gegevens (data), te realiseren door een goede controle bij de invoer (data entry) en gecontroleerd beheer van de gegevens[17]. Naast de borging van de integriteit tijdens het beheer wordt de integriteit ook gewaarborgd door de *transactie-integriteit*.
De integriteit tijdens het beheer wordt gewaarborgd binnen de beheer- en beveiligingsprocessen. Het waarborgen van de transactie-integriteit moet worden meegenomen in Privacy by Design. In het ontwerp moet daarom rekening gehouden worden met de regels voor transactiemanagement. Bedenk daarbij dat transactiemanagement een bredere scope heeft dan een database. De scope omvat in het kader van de privacy de integriteit van de gehele set van persoonsgegevens van een persoon, dus alle vormen van opslag van persoonsgegevens van een persoon. Dit kunnen meerdere (gestructureerde) databases zijn, maar ook meerdere bestanden met ongestructureerde gegevensopslag betreffen.

De regels voor transactiemanagement (ACID): zonder een waterdichte set van regels kunnen (persoons)gegevens, bijvoorbeeld opgeslagen in een database, gemakkelijk gegevens bevatten die inconsistent zijn. Bij het bewaren van (persoons)gegevens wordt daarom geacht aan de ACID-eisen te voldoen[18]:

- **Atomair:** Een transactie wordt altijd volledig uitgevoerd. Als een transactie uit meerdere onderdelen bestaat, dan zijn na afloop van de transactie ofwel *alle* onderdelen uitgevoerd, ofwel *geen* van de onderdelen.
- **Consistent:** Na uitvoering van een transactie is de database consistent, dat wil zeggen dat alle regels die zijn vastgelegd voor de gegevens gelden.
- **Geïsoleerd:** Transacties worden geïsoleerd van elkaar uitgevoerd, dat wil zeggen dat transacties die tegelijkertijd worden uitgevoerd geen inzicht hebben in elkaars tussenresultaten.
- **Duurzaam:** Na de uitvoering van een transactie zijn de gegevens duurzaam vastgelegd.

Om te achterhalen of in voldoende mate aan de ACID-principes wordt voldaan moeten in runtime testen worden uitgevoerd, deze staan beschreven in Bijlage 1: Testen op ACID-eisen.

Realiseren van de consistentie door transactiemanagement: veelal zijn meerdere gebruikers of processen actief op een enkele gegevensopslag. Ontwikkelomgevingen hebben blueprints of modellen voor het transactiemanagement[19]. De scope van de transactie betreft altijd één applicatie. De integriteit over de transacties vanuit meerdere applicaties, veelal op meerdere databases, moet een aandachtspunt zijn tijdens het ontwerp.

Realiseren van de consistentie door gegarandeerde levering: bij het uitwisselen van gegevens via services moet bewaakt worden dat de gegevensuitwisseling daadwerkelijk heeft plaatsgevonden. Voor het bewaken kan gebruik gemaakt worden van een standaard: WS-Reliable Messaging[20].

Realiseren van de consistentie door afscherming van transacties: bij het uitwisselen van gegevens kunnen gegevens gewijzigd worden; het is daarom van belang deze gegevensuitwisseling af te schermen. Dit kan door het fysiek of elektronisch beveiligen van de verbinding of netwerk, maar veelal is het beter hier te kiezen voor encryptie van de uitwisseling zelf. Dit kan door middel van:

- Gebruik van HTTPS oftewel HTTP over TLS (zie SSD [10] en SSDm [9]);
- Gebruik van de standaard WS-SecureConversation[21].

[17] Afgeleid van definitie "Data integrity" uit: Hein van Steenis - Computable ICT woordenboek, 2003/7.
[18] https://nl.wikipedia.org/wiki/Transactie_(dataopslag)
[19] http://www.javaworld.com/article/2076126/java-se/transaction-management-under-j2ee-1-2.html en https://msdn.microsoft.com/library/bb738523(v=vs.100).aspx.
[20] https://en.wikipedia.org/wiki/WS-ReliableMessaging
[21] https://en.wikipedia.org/wiki/WS-SecureConversation

Verkeerde conclusies over een persoon op basis van inconsistente (persoons)gegevens
als gevolg van verkeerd of incompleet uitgevoerde transacties
worden voorkomen door het hanteren ACID regels voor transactiemanagement.

6.5 Het voorkomen van onjuiste redenatie

Het toepassen van een verkeerde bedrijfslogica (bedrijfsregels) op persoonsgegevens kan onbedoelde uitkomsten tot gevolg hebben en daarmee leiden tot foutieve informatie of besluiten over iemand. Het is zowel in het belang van de betrokkene als de verwerkende organisatie dit te voorkomen. Beiden dienen in staat te zijn de onjuistheid en onnauwkeurigheid van de gegevens te voorkomen, te constateren en zo nodig te corrigeren.

6.5.1 Het ontwikkelen van de redenatie

Een onjuiste redenatie leidt tot verkeerde conclusies over de betrokkene. Dit kan leiden tot negatieve consequenties voor de betrokkene. Het voorkomen hiervan vraagt om regels bij het ontwikkelen van de logica:

1. De gehanteerde logica past binnen de doelbinding en daarmee binnen de bij de ontvangst van de gebruikte gegevens aan de betrokkene aangegeven informatie (U.05).
2. De gehanteerde logica is niet strijdig met de elders, in andere verwerkingen, gehanteerde logica. Het geheel aan gehanteerde logica is samenhangend en past binnen de menselijke maat, zodat de betekenis ervan aan de betrokkene is uit te leggen. Zodoende kan aan de in criterium C.02 vereiste transparantie worden voldaan.
3. De gehanteerde logica is nauwkeurig bepaald en gebaseerd op een interpretatievrije analyse van de wet- en regelgeving en de doelbinding (criteria U.01 en U.03).
4. De gehanteerde logica maakt gebruik van gegevens, waarvan de betrouwbaarheid is bepaald (U.03).
5. De kwaliteit van de gehanteerde logica wordt beheerd in een PDCA-cyclus; de logica is daardoor aanpasbaar (onderhoudbaar) (U.03).
6. De gehanteerde logica is in een voor de betrokkenen begrijpbare taal (in een "declaratieve taal") beschreven (C.02) en kan door de business kan worden gecontroleerd op juistheid en consistentie met andere logica (U.03). Omgekeerd wordt er geen gebruik gemaakt van een logica, die niet in een voor de betrokkene begrijpbare taal kan worden beschreven (U.05).

Voor de analyse om te komen tot de gehanteerde logica en het beheer ervan zijn hulpmiddelen voorhanden:

- **Business Rule Management**: Business Rule Management (BRM) omvat de geautomatiseerde ondersteuning die nodig is voor de analyse om te komen tot bedrijfslogica en de deze logica en de uitleg ervan integraal te beheren. Het geautomatiseerde tool bevat een Business Rule Engine BRE). Een BRE is in staat om ingevoerde gegevens te evalueren tegen de geldende regels die zijn vastgelegd in een regelrepository.
- **Data Management Platforms**: Data management platforms (DMP) ondersteunen geautomatiseerde profiling, bijvoorbeeld voor adverteren. Hoewel DMP de kwaliteit van profiling kan verbeteren, kent profiling altijd een groot risico voor de privacy.

De kans op een onjuiste redenatie in de logica en
daarmee de kans op negatieve consequenties voor de betrokkene
wordt verminderd door het gebruik van kwaliteitsregels bij het ontwikkelen van de logica.

6.5.2 Persona management

Persona management kan helpen te voorkomen dat een onjuist profiel wordt opgebouwd. Dit gebeurt door mensen en bedrijven te helpen bijhouden welke gegevens ze delen of communiceren en in welke rol (persona) ze die delen, dus bijvoorbeeld als betrokkene, baas of als medewerker. Omgekeerd kan op basis van de persona bepaald worden of toegang gegeven mag worden tot bepaalde informatie.

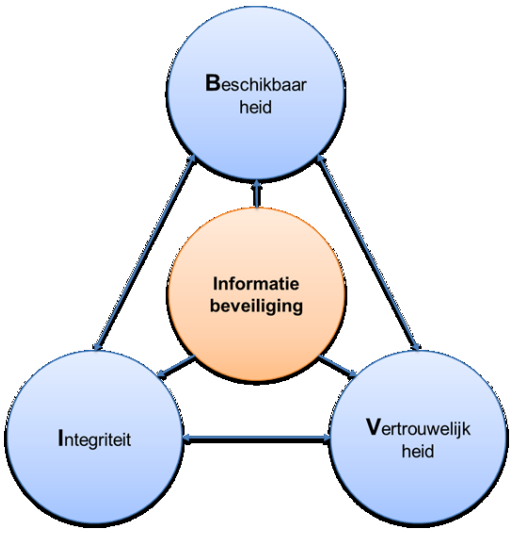
Voor de gebruiker wordt de scheiding tussen hun persoonlijke en zakelijke digitale leven gemakkelijker, omdat het voor de gebruiker voorkomt dat zij informatie krijgen die niet bij de persona/rol past die zij op dat moment hebben. Omgekeerd biedt het de dienstenaanbieder de mogelijkheid alleen die informatie te delen (en te verbeteren) die past bij de persona/rol van de gebruiker.

Het opbouwen van juiste profielen van een persoon en het gebruik ervan vraagt om een zorgvuldige scheiding van rollen die een persoon kan hebben.

7 Beveiligen van persoonsgegevens

De doelstellingen van informatiebeveiliging zijn het waarborgen van de beschikbaarheid, integriteit en de vertrouwelijkheid van de (verwerking van de) gegevens en daarmee ook die van persoonsgegevens. Informatiebeveiliging vult een belangrijk deel van het ACT-doel 'Afscherming' in. Dit betekent echter niet dat informatiebeveiliging per definitie ook de maatregelen neemt die gericht zijn op privacybescherming en daarbij op het waarborgen van de belangen van de betrokkene.

Soms stelt privacybescherming aanvullende eisen aan het waarborgen van de beschikbaarheid, integriteit en de vertrouwelijkheid.



Maatregelen voor informatiebeveiliging bestaan uit organisatorische, technische en fysieke maatregelen die gebaseerd zijn op een risicoanalyse. Belangrijk is nu dat daarbij de privacy-risico's in de risicoanalyses worden meegenomen, met extra aandacht voor bijzondere persoonsgegevens en uniek identificerende gegevens.

Om er zeker van te zijn dat de juiste maatregelen zijn of worden getroffen is het nuttig om na te gaan waar de verschillen kunnen zitten tussen de al dan niet door informatiebeveiliging genomen maatregelen en de eisen die vanwege de privacybescherming nodig zijn.

	Eisen binnen de BIV-doelen	Eisen binnen de ACT-doelen
Beschikbaarheid	De beschikbaarheid van de bedrijfsvoering	Blijvend een actueel en accuraat beeld van de betrokkene
Integriteit	Zodat de bedrijfsvoering niet in gevaar komt	Zodat er geen verkeerde conclusies over de betrokkene worden getrokken.
Vertrouwelijkheid	Afscherming van "onbevoegden"	Afscherming van eenieder die geen toegang nodig heeft voor de uitvoering van zijn taak (rol-, taak- en tijdsafhankelijk).
	Afscherming van ongeoorloofde toegang	Voorkomen van het gebruik van de gegevens voor andere doelen dan de vastgelegde doelbinding.
	Toegang moet te herleiden zijn tot een natuurlijk persoon	Toegang moet rolgebaseerd zijn, waarbij de verwerking door de bewerker schriftelijk is geregeld[22].
	Voldoen aan de standaard beveiligings-eisen.	Hogere eisen aan de afscherming van bijzondere persoonsgegevens.

7.1 Een passend beveiligingsniveau

De beveiliging van persoonsgegevens vraagt om passende maatregelen. U.04/02 definieert wanneer een passend niveau van beveiligen wordt geboden. Kort gezegd wordt een passend niveau geboden, wanneer er aantoonbaar technische, organisatorische en fysieke beveiligingsmaatregelen zijn genomen, die gebaseerd zijn op een actuele risicoanalyse, waarbij rekening is gehouden met de aard en de context van de persoons-gegevens en de maatregelen periodiek worden geëvalueerd en bijgehouden. Daarmee kan de op risico gebaseerde aanpak van bijvoorbeeld de NEN ISO 27001 gehanteerd worden en kan ISO 27002 gezien worden

[22] Dit kan in een bewerkersovereenkomst of in een arbeidsovereenkomst.

als dagelijkse en daarbij passende beveiligingspraktijk. De van de ISO normen afgeleide baselines, zoals de Baseline Informatiebeveiliging Rijksoverheid (BIR) of de BIG voor de gemeenten kunnen voor de overheid als passende beveiligingspraktijk worden beschouwd.

Zoals in criterium U.04 aangeeft moet met de aard van de persoonsgegevens meetellen bij wat als passend gezien kan worden. Bijzondere persoonsgegevens zijn naar hun aard vertrouwelijker dan 'gewone' persoonsgegevens en moeten daardoor zwaarder beveiligd worden[23].

Met de huidige stand van de techniek (anno 2016) worden de volgende maatregelen doorgaans als passend gezien:

1. Authenticatie op een vertrouwde locatie, zoals een werkplek[24] binnen een beveiligd kantoor en op een beveiligd netwerk[25], vindt minimaal op basis van een kenniskenmerk (wachtwoord) plaats.
2. Authenticatie op een niet-vertrouwde locatie, zoals een werkplek thuis of in een openbare ruimte, of via een niet vertrouwd netwerk[26], vereist naast het kenniskenmerk ook een bezitskenmerk.
3. Persoonsgegevens die worden verstuurd over het bedrijfseigen beveiligde netwerk worden bij voorkeur versleuteld; buiten het eigen beveiligde netwerk, zoals Internet, worden ze altijd versleuteld. Dit geldt ook op draagbare media.
4. Services[27] die persoonsgegevens verwerken of aanbieden zijn niet te benaderen zonder autorisatie en authenticatie, bijvoorbeeld door het gebruik van certificaten.
5. Fysieke en logische maatregelen schermen de verwerking van de persoonsgegevens af, bijvoorbeeld door servers in afgesloten ruimtes te plaatsen en systemen/componenten te 'hardenen'[28].
6. De toegang tot persoonsgegevens door systeembeheerders wordt vastgelegd (tijd en raadpleger worden gelogd).
7. De toegang en het gebruik wordt vastgelegd (tijd, raadpleger, proces, en resultaat worden gelogd).

In aanvulling op de maatregelen voor de 'gewone' persoonsgegevens worden de volgende maatregelen voor bijzondere persoonsgegevens doorgaans als passend gezien:

8. Authenticatie vindt naast het kenniskenmerk altijd ook op basis van een bezitskenmerk plaats.
9. Bijzondere persoonsgegevens worden, ook als ze verstuurd worden over het bedrijfseigen beveiligde netwerk, versleuteld.

Daar waar tekortkomingen geconstateerd worden moeten de aanvullende eisen vanuit privacy worden ingevuld.

1. **Exclusiviteit en integriteit**:
   - Encryptie van persoonsgegevens (versleuteling)
   - Anonimisering
2. **Afspraken met derden**:
   - Bewerkersovereenkomst, inclusief processen, controle en maatregelen;
   - Het opstellen, implementeren en handhaven van het beveiligingsbeleid;

Bij voorkeur is de informatiebeveiliging ingeregeld volgens de NEN-ISO 27001/27002 en de afgeleide overheidsnormen (BIR, BIG, BIWA, …), omdat dit de standaard is voor 'adequate' beveiliging. Van belang is om te weten dat de BIR en de BIG de NEN-ISO normen niet vervangen, maar een *praktische uitvoeringshandleiding* vormen: toets altijd aan de *volledige* NEN-ISO normen!

[23] Paragraaf 1.1.1 Privacy Baseline
[24] Van de werkplek wordt minimaal verwacht dat de werkplek beschermd is tegen onrechtmatig gebruik.
[25] Een beveiligd netwerk is een netwerk, waarvan het netwerkverkeer niet toegankelijk is voor onbevoegden.
[26] Een onbeveiligd netwerk is bijvoorbeeld Internet of een netwerk van derden.
[27] Met een service wordt hier een service bedoeld, zoals die voorkomt in een Service Georiënteerde Architectuur (SGA ofwel SOA)
[28] Hardenen is het beperken van de communicatiemogelijkheden tot een strikt noodzakelijk minimum. Dit kan bijvoorbeeld door onnodige interfaces onbereikbaar te maken door ze te verwijderen of uit te schakelen.

Het passend zijn van beveiligingsmaatregelen is gebaseerd op risicoanalyses,
op wat gangbaar is in de markt en op wat als de 'stand van de techniek' wordt gezien.
Het blijvend voldoen aan de stand van de techniek vraagt om een cyclisch PDCA-proces.

7.2 Identity en Access Management (IAM)

Identity en Acces Management (IAM) is een van de belangrijkste onderdelen van de beveiliging van persoonsgegevens. IAM moet waarborgen dat:

1. Alle verwerkingen herleidbaar zijn tot natuurlijke personen.
2. Voor al deze verwerkingen het need-to-know - en het doelbindingsprincipe (U.01) wordt toegepast.

Je regelt dit met een authenticatieservice en een autorisatieservice.

7.2.1 Authenticatieservice

De authenticatieservice heeft tot doel alle verwerkingen te kunnen herleiden tot natuurlijke personen. Voor de herleidbaarheid tot natuurlijke personen zijn twee of drie stappen nodig:

1. **Identificatie:**
   Identificatie is het kenbaar maken van de identiteit van een persoon. Dit gebeurt door middel van een identificatiebewijs en persoonlijk contact. Ook kan er voor gekozen worden uit te gaan van identificatie op basis van een authenticatiemechanisme, waarbij al reeds identificatie heeft plaatsgevonden.

2. **Authenticatie van de persoon:**
   Nadat een identiteit is vastgesteld moet in het vervolg altijd worden vastgesteld dat de persoon die een handeling wil verrichten *op grond van die identiteit* daadwerkelijk degene is die achter de identiteit schuilgaat. Deze controle is meervoudig en geschiedt (in zijn simpelste en op dit moment meest gebruikte vorm) door het matchen van de bij de identiteit behorende gebruikersnaam en wachtwoord.

3. **Authenticatie van een service of applicatie:**
   Voor de verwerkingen die in opdracht van een natuurlijk persoon[29] door een service of applicatie worden uitgevoerd is altijd authenticatie van de service of applicatie nodig. Doordat de service of applicatie in opdracht van een natuurlijk persoon wordt uitgevoerd is deze persoon de bewerker van de persoonsgegevens.

Iedere verwerking dient terug te leiden te zijn tot een natuurlijke persoon.

7.2.2 Autorisatieservice

Een autorisatieservice heeft tot doel verwerkingen alleen toe te laten als een taak uitgevoerd moet worden die past binnen de doelbinding en de taken die aan een bewerker zijn toegewezen. Het toewijzen van taken gebeurt op basis van de functie van deze bewerker en de rol die hij of zij binnen die functie heeft[30].
Dit vereist de volgende stappen:

1. Per verwerking wordt bepaald welke groepsrechten nodig zijn. Dit gebeurt per applicatie en wordt veelal geadministreerd in directory services[31].
2. De groepsrechten worden gekoppeld aan de rollen binnen de functies van de medewerkers.

[29] Veelal zal deze natuurlijke persoon dit namens bijvoorbeeld het bestuur van een bedrijf of organisatie doen.
[30] Met deze persoon zijn vooraf de afspraken vastgelegd over bijvoorbeeld de vertrouwelijkheid in een bewerkersovereenkomst.
[31] Een directoryservice is een dienst die gegevens over de delen/componenten in een computernetwerk beheert. De gegevens worden daarbij in een hiërarchische structuur bewaard, waarbij ook de relaties tussen gegevens worden bewaard, zodat het overzicht behouden blijft.

Indien het (bij stap 2) een groot aantal autorisaties betreft en er dus een groot aantal koppelingen tussen de rechten en de medewerkers moeten worden gelegd, vraagt het aantoonbaar correct uitgeven van rechten om een geautomatiseerde ondersteuning. Wanneer niet langer aan de condities van de bewerkersovereenkomst wordt voldaan, bijvoorbeeld bij verandering van functie of ontslag, moeten de rechten daarbij automatisch vervallen.
Deze zaken zijn mogelijk en te managen met een Role Based Access Control (RBAC) systeem, waarin standaard-autorisaties aan rollen zijn gekoppeld. Medewerkers, en dus ook bewerkers, kunnen dan door middel van een passende rol eenvoudig aan passende toegangsrechten worden gekoppeld. De rol bepaalt welke verwerkingen passen binnen de doelbinding en de taken van de bewerker aan wie de rol is toegekend.

Iedere verwerking dient te passen binnen de doelbinding en de taken die aan een bewerker zijn toegewezen.

7.2.3 Toestemmingmanagement

Toestemmingmanagement (Consent Management) is een systeem, waarbij de persoon, waarover de persoonsgegevens gaan (de betrokkene), toestemming geeft informatie te delen of in te zien. Hierbij kan worden aangegeven voor welk doel en in welke situatie welke informatie toegankelijk kan worden gemaakt.
De betrokkene kan daardoor per gegevensverwerking/ situatie bepalen welke persoonsgegevens mogen worden ingezien en gebruikt. Opslag van de persoonsgegevens vindt dan niet plaats door de bewerker van de gegevens, maar door of onder controle van de betrokkene zelf.

Middels toestemmingsmanagement heeft de betrokkene controle over zijn persoonsgegevens en de doelen waarvoor ze worden gebruikt.

7.3 Bewaren van persoonsgegevens

Het bewaren van persoonsgegevens is meer dan het simpelweg opslaan van gegevens. Het bewaren van persoonsgegevens is op zich al een vorm van verwerken van persoonsgegevens. Bij het bewaren van persoonsgegevens kunnen inrichtingsprincipes gehanteerd worden, zodat eenvoudiger aan criterium U.06: "Bewaren van persoonsgegevens" kan worden voldaan. Hierbij wordt gekeken naar de verschillende levensfases van de gegevens.
Om aan criterium U.06 te kunnen voldoen kunnen technologieën ten behoeve van veilige opslag worden ingezet (zie paragraaf 7.5). Daarnaast moet bij het ontwerpen van de gegevenshuishouding gekeken worden naar:

1. Het beheersbaar bewaren;
2. Het bepalen van de bewaartermijn;
3. Het vernietigen.

7.3.1 Beheersbaar bewaren: Single point of truth

De omvang van de data neemt constant toe. Dit vraagt om het snel en efficiënt kunnen vinden van de juiste data. Dit vraagt om een gerichte aanpak. Discussies over welke informatie betrouwbaar is kunnen worden voorkomen door het bieden van de "single point of truth". Single point of truth waarborgt de vindbaarheid, ontsluiting van informatie en het terugdringen van redundantie en het gebruik onjuiste gegevens. Naast het vergroten van de kwaliteit van de persoonsgegevens (U.03) verbetert het de transparantie (doel: T van de ACT-doelen) en verbetert het de beveiliging (U.04).

Single point of truth (geen duplicaten) maakt een kwalitatieve en transparante gegevensverwerking mogelijk

Indien er, bijvoorbeeld vanuit beschikbaarheids- en performanceoverwegingen, voor gekozen wordt persoonsgegevens op meerdere plaatsen op te slaan, worden deze duplicaten tot een hoogst noodzakelijk minimum beperkt om het overzicht te behouden en het beheer te beperken. Om de kwaliteit van de gegevens te kunnen bepalen en te bewaken is het van belang te weten welke registratie de authentieke registratie is

(single point of control). Het wijzigen van duplicaten moet voorkomen worden: alleen de authentieke registratie kan worden aangepast.

Van gerepliceerde gegevens is altijd bekend wat de authentieke registratie is (single point of control).

7.3.2 De bewaartermijn van de gegevens

De Avg eist dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is om het doel te bereiken (U.06/01) en daarna verwijderd, vernietigd of geanonimiseerd worden (U.06/02). Voor sommige persoonsgegevens is er in sectorspecifieke wetgeving een bewaartermijn vastgesteld; in dat geval geldt die bewaartermijn in plaats van de bewaartermijn van de Avg.
Overheidsorganen zijn op grond van de Archiefwet 1995 verplicht in een selectielijst vast te leggen welke archiefbescheiden in aanmerking komen voor bewaring en welke voor vernietiging [11]. Een selectielijst regelt welke categorieën archiefbescheiden op termijn vernietigd moeten worden, en welke voor altijd bewaard blijven. Blijvend te bewaren stukken brengt uw organisatie uiteindelijk over naar een archiefbewaarplaats.

De selectielijst geeft (als instrument van de Archiefwet) de bewaartermijnen voor persoonsgegevens aan.

Het bepalen en vastleggen van de bewaartermijn per gegeven en het gebruik van de selectielijst kan in een procedure worden vastgelegd. Door deze procedure door of samen met gegevensmanagement te laten uitvoeren, kan gewaarborgd worden dat de bewaartermijn voorafgaand aan de opslag wordt bepaald.

7.3.3 Het vernietigen van de gegevens

Het verwijderen, vernietigen en anonimiseren van persoonsgegevens is relatief eenvoudig als gegevens duidelijk voor één doel en één verwerking zijn bewaard. De technische maatregel 'gegevens wiping', zoals in paragraaf 7.5.6 beschreven, laat zien hoe gegevens vernietigd kunnen worden. Wel moet duidelijk zijn waar zich de gegevens bevinden, inclusief de backup bestanden en de eventuele archieven, zodat daadwerkelijk *alle* gegevens vernietigd kunnen worden.

- Niet in alle gevallen is vernietiging mogelijk, bijvoorbeeld als de gegevens gebruikt worden door meerder verschillende doelen en verwerkingen of wanneer de gegevens worden bewaard op een opslagmedium, waarvan de gegevens niet verwijderd kunnen worden, zoals op en "read only" gegevensdrager bijvoorbeeld een CD of DVD. Ook archieven zijn vaak "read only" en hebben dan niet de mogelijkheid gegevens te verwijderen.
- Indien gegevens voor meerdere doelen gebruikt worden is het van belang dat een juiste granulariteit in het datamodel is gehanteerd (zie paragraaf 4.3.1). Het is dan mogelijk (de toegang tot) delen van de gegevensverzamelingen te verwijderen, terwijl deze gegevens toegankelijk blijven voor verwerkingen waarvoor de bewaartermijn van de gegevens nog niet zijn verlopen. Ook kan ervoor gekozen worden de gegevens te anonimiseren, zodat zij niet meer als persoonsgegeven gebruikt kunnen worden, maar wel bijvoorbeeld voor statistische doeleinden.
- Indien alle bewaartermijnen zijn verlopen is er geen legitimering voor het bewaren van de gegevens en moeten de gegevens vernietigd worden.
- Bedenk dat ook de betrokkenen opdracht kunnen geven hun persoonsgegevens te laten vernietigen. In bepaalde gevallen (zie U.01) moet deze opdracht ook uitgevoerd kunnen worden, namelijk als de betrokkene zijn toestemming voor de gegevensverwerking intrekt of als hij zich verzet tegen gebruik voor direct marketing. In beide gevallen moet de gegevensverwerking direct stopgezet worden en moeten de persoonsgegevens worden verwijderd. Houd in het ontwerp van het systeem rekening met deze mogelijkheid als extra functionaliteit.

Het rekening houden met het vernietigen van persoonsgegevens komt terug in de verschillende ontwikkelfasen en ontwerpkeuzes en begint al bij de keuze van het wel of niet verzamelen van de persoonsgegevens.

7.4 Doorgifte persoonsgegevens

Organisaties werken vaak in ketens. Ketens vormen een aaneenschakeling van partijen die samenwerken en daarbij (persoons)gegevens delen of wisselen. Bij het ontwerpen van een verwerking is het van belang een beeld te hebben van de partijen die toegang krijgen tot de persoonsgegevens binnen die (keten)verwerking. Met ieder van deze partijen moeten afspraken gemaakt worden of moeten bestaande afspraken gecontroleerd worden op de vereisten, zoals die in criterium U.07 zijn beschreven.

- Belangrijk is hierbij niet alleen naar de zogenaamde horizontale ketens32 te kijken, maar ook naar de verticale ketens. Verticale ketens beginnen bij de organisatie (of afdeling) met de verantwoordelijke voor de gegevensverwerking en lopen via de eventuele interne technische beheerders en gecontracteerde netwerkleverancier en hostingpartij en eindigt bij de onderaannemers van de gecontracteerde leveranciers.
- Wees erop bedacht dat, hoewel een gecontracteerde leverancier zich binnen de EER kan bevinden, diens eventuele onderaannemers zich buiten de EER kunnen bevinden. Dat kan - letterlijk - heel ver gaan en ook gelden voor de eventueel gecontracteerde onderaannemers (bewerkers) van partijen in een horizontale keten, aan wie gegevens worden doorgegeven. Voor leveranciers en doorgifte buiten de EER gelden aanvullende vereisten (U.07/03 t/m U.07/06)

Bij het ontwerp van de verwerking wordt nagegaan of de partijen
die zich in zowel de horizontale ketens als de verticale ketens bevinden
voldoen aan de criteria voor de doorgifte van persoonsgegevens (U.07).

7.4.1 Contractering van ketenpartijen

Ketenpartijen die gegevens verwerken van of namens de organisatie (in een zogenaamde horizontale keten) of partijen die persoonsgegevens hosten of op een andere wijze systemen beheren (in een zogenaamde verticale keten) worden allen aangemerkt als bewerker. Voor deze bewerkers gelden dezelfde eisen als voor de organisatie waarvoor ze dat doen. (zie U.07/02)
Indien een partij het doel van en de middelen voor de verwerking van persoonsgegevens zelf vaststelt is deze partij zelf verantwoordelijk voor de gegevens verwerking. Omdat de partij die de gegevens doorgeeft, voor de doorgifte verantwoordelijk is, met deze partij ervoor zorgen dat de onderlinge verantwoordelijkheden worden/ zijn vastgelegd (zie U.07/01).

De overeenkomsten met de andere verwerkingsverantwoordelijke moeten informatie vastleggen conform de vereisten in het indicator U.07/01 en die met een verwerker conform de vereisten in het indicator U.07/02. Indien het een ketenpartij of een onderaannemer van de ketenpartij buiten de Europese Economische Ruimte (EER) betreft gelden aanvullend de vereisten in het indicator U.07/03 t/m U.07.06.
In "Grip op beveiliging in inkoopcontracten" [5] wordt een 'menukaart' gegeven voor de vastlegging van de bescherming van de privacy en informatieveiligheid. In de "Handreiking Beveiligingsbeleid Clouddiensten" [12] wordt beschreven hoe je afspraken maakt met dienstenleveranciers in een verticale keten.

Ketensamenwerkingen vragen om contracteringen van ketenpartijen.
Hierbij moet aandacht zijn voor horizontale én verticale ketens
en of de verwerking wel of niet (door een partij van) buiten de EER wordt uitgevoerd.

7.4.2 Onderling vertrouwen

Bij de doorgifte van persoonsgegevens kan de vertrouwensrelatie met degene waarmee informatie wordt uitgewisseld de ontwerpkeuzes beïnvloeden. Weinig vertrouwen vraagt om meer aantoonbaar beschermende maatregelen en/of controles of beperking van de toegang tot - of de uitwisseling van persoonsgegevens. Belangrijk daarbij is wel dat het vertrouwen niet gebaseerd is op blind vertrouwen. De partijen waaraan de persoonsgegevens worden doorgegeven moeten het vertrouwen verdienen en behouden. Dit vraagt om een structurele dialoog over de risico's, de genomen maatregelen en de weerbaarheid; "vertrouwen moet ook

[32] Een voorbeeld van een horizontale keten is een keten van overheidspartijen, zoals de SUWI-keten.

gestaafd kunnen worden". Een juist onderling vertrouwen voorkomt het nemen van onnodige maatregelen en onnodige controles.

Helderheid over onderling vertrouwen is vereist om te komen tot passende maatregelen.

7.4.3 Koppelingen voor de doorgifte van en toegang tot persoonsgegevens

De verwerking van persoonsgegevens vindt doorgaans niet binnen één verantwoordelijkheidsdomein plaats. Vaak vindt de verwerking van de gegevens plaats in een keten, waarbij de verschillende vormen van verwerking van de persoonsgegevens door derden wordt uitgevoerd. Hierbij kan een veelheid aan koppelingen ontstaan met derde partijen. Twee maatregelen worden in het bijzonder aanbevolen:

- Het toestaan van een externe koppeling en de doorgifte van persoonsgegevens vragen om een goedkeuringsprocedure; een certificeringprocedure kan hier onderdeel van uitmaken.
- Door de convergentie van de verkeerstromen over één koppelvlak en daarbuiten geen koppelingen toe te staan is monitoring van de verkeersstromen en bewaking van de doelbinding van de gegevensuitwisseling eenvoudig(er) mogelijk en kunnen zo onrechtmatige gegevensuitwisselingen aan partijen, die niet aan de eisen van de doorgifte voldoen, beter voorkomen worden.

Convergentie van verkeersstromen met persoonlijke gegevens naar één koppelvlak maakt de doorgifte en toegang beter beheersbaar.

7.4.4 Locatie van de opslag en verwerking

Het beheren van persoonsgegevens en de technische systemen voor de verwerking van de persoonsgegevens door een beheerpartij, zodat de gegevens beschikbaar en afgeschermd zijn, kent een groot aantal taken. Deze taken worden aangeduid als 'technisch beheer'. *Ook het technisch beheer valt onder de noemer verwerking*, zoals de Avg het begrip hanteert. Daarmee vallen ook alle vormen van technisch beheer onder het regime van de Avg en moeten afspraken met alle partijen die zijn betrokken bij het technisch beheer contractueel vastgelegd worden, inclusief afspraken over het hanteren van een bewerkersovereenkomst. Dit geldt niet alleen voor de locatie van de opslag van de persoonsgegevens, maar ook voor de locaties waar of waarvandaan de beheeractiviteiten plaatsvinden. Beheeractiviteiten bij grotere beheerpartijen kunnen plaatsvinden vanuit de gehele wereld, dus van buiten de EER. Hiervoor gelden aanvullende eisen bovenop die voor binnen de EER (zie paragraaf 7.4.1)

De vereisten voor doorgifte worden naast de locatie van de opslag van persoonsgegevens ook bepaald door de locatie waar of waarvandaan technisch beheer wordt gepleegd.

7.4.5 Pseudonimisering

Door persoonsgegevens met een bepaald algoritme te versleutelen ontstaan versleutelde gegevens, die een pseudoniem zijn van de oorspronkelijke gegevens. Door voor dat persoon steeds hetzelfde algoritme te gebruiken wordt voor dat persoon van een persoonsgegeven altijd hetzelfde pseudoniem berekend. Daarin onderscheidt pseudonimiseren zich van anonimiseren, doordat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon kunnen worden gekoppeld (mits de juiste technische en organisatorische maatregelen zijn genomen), maar wel gecombineerd worden.
Doordat deze informatie over dit persoon is te combineren met de pseudoniemen uit verschillende bronnen is bijvoorbeeld verwerking voor wetenschappelijk of historisch onderzoek of statistische doeleinden mogelijk, zonder dat dat persoon is te identificeren.

7.4.6 Openheid door ketenpartijen

Zoals eerder gesteld blijft de verstrekker van de persoonsgegevens eindverantwoordelijk voor de rechtmatige verwerking ervan als hij de oorspronkelijke verantwoordelijke is en voor zolang de gegevens niet zijn overgedragen aan een nieuwe verantwoordelijke partij. Om deze verantwoordelijkheid te kunnen invullen is openheid nodig van alle ketenpartijen over hun beleid en genomen maatregelen om de privacy te waarborgen.

Ook openheid door het delen van *informatie over risico's en incidenten* vergroot de weerbaarheid van de keten, zodat de privacy beter beschermd kan worden. Hoe de weerbaarheid contractueel kan worden vastgelegd staat onder de noemer "weerbaarheid" beschreven in "Grip op beveiliging in inkoopcontracten" [5].

Het vergroten van de weerbaarheid tegen privacy-incidenten vraagt om openheid over de privacybescherming, inclusief informatieuitwisseling over risico's en incidenten.

Openheid over privacybescherming gaat verder dan alleen het informeren over het beleid en de genomen maatregelen ten aanzien van de privacybescherming. Het beschermen van de privacy betreft ook het waarborgen van de gegevenskwaliteit (U.03). Indien gegevens onjuist of onvolledig zijn dan is het van belang dat de authentieke bron hiervan op de hoogte wordt gebracht en deze de andere ketenpartijen die gebruik maken van deze gegevens op de hoogte stelt.
In het ontwerp van de keten en de gegevensuitwisselingen moet er daarom aandacht zijn voor het kunnen melden van onjuiste gegevens bij de authentieke gegevensbron(nen).

De zorg voor de juistheid van persoonsgegevens is niet beperkt tot één partij, maar is een ketenverantwoordelijkheid en moet daarom meegenomen worden in het ontwerp en de gegevensuitwisselingen.

7.5 Technologieën voor veilige opslag

7.5.1 Database-encryptie

Database-encryptie wordt gebruikt om de vertrouwelijke gegevens in een database te beschermen. Dit kan door het versleutelen van de gehele database of het versleutelen van delen of velden. Door sleutelbeheer volledig apart te houden van het databasebeheer, voorkom je dat beheerders altijd rechtstreekse toegang hebben tot de vertrouwelijke gegevens tijdens hun beheerwerk.

Database-encryptie kan op verschillende manieren worden ingevuld.
Een passende wijze is gebaseerd op een risicoanalyse.

7.5.2 Limited Disclosure Technology

Limited Disclosure Technology draagt bij aan de bescherming van de privacy door te regelen dat alleen die persoonsgegevens met een dienstenleverancier gedeeld worden, die nodig zijn voor het uitvoeren van de dienst. De techniek maakt gebruik van cryptografische technieken. Na gebruik door een dienstenleverancier worden de gegevens overdragen aan een vertrouwde derde partij. Deze partij beheert de gegevens en waarborgt de authenticiteit en integriteit van de gegevens. Dit beperkt de mogelijkheid van profiling en het volgen van gebruikers, het delen van gegevens met anderen en zelfs met de dienstenleverancier. Dit kan zo, omdat alleen gevraagd hoeft te worden aan de vertrouwde partij of aan een criterium is voldaan, zoals een bijvoorbeeld leeftijdseis, zonder dat het gegeven zelf gedeeld hoeft te worden.

Het beperken van het delen van persoonsgegevens verlaagt het risico op misbruik.

7.5.3 Tokenization

Bij tokenization wordt een vertrouwelijk gegeven beveiligd door het te vervangen het gegeven door een niet-gevoelige waarde. Bij het omzetten van het gegeven wordt gebruik gemaakt van encryptietechnieken met geheime sleutels. Deze niet-gevoelige waarde wordt aangeduid als "token". Een token kan veilig worden gedeeld.
Er kan voor gekozen worden het vertrouwelijke gegeven weer zichtbaar te maken met het proces van "de-tokenization", waarbij het token wordt ontcijferd. Veelal wordt er echter voor gekozen het token niet te laten ontcijferen. Controle of een gegeven, bijvoorbeeld een creditcardnummer, juist is, gebeurt door het te controleren gegeven met dezelfde sleutel om te zetten in een token en de tokens met elkaar te vergelijken. Tokenization kan op verschillende manieren worden geïmplementeerd: in eigen huis, uitbesteed of een hybride

model. Hoe minder in eigen huis gebeurt, des te minder vertrouwelijke gegevens in huis zijn en daar beveiligd moeten worden. Voor tokenization bestaat een standaard: de PCI Data Security Standard (DSS). Deze standaard beschrijft de tokenization zelf en een audit voor het gebruik van (de-)tokenization.

Tokenization maakt een veilige verwerking van persoonsgegevens mogelijk, zonder het persoonsgegeven zelf te delen.

7.5.4 Datamasking

Datamasking is een methode om gegevens, zoals persoonsgegevens, te verbergen. Het verbergen is mogelijk door data geheel of gedeeltelijk ontoegankelijk te maken, te verwijderen of te veranderen. Hierdoor wordt het niet meer mogelijk te achterhalen over wie een gegeven gaat. Dit wordt dan ook wel aangeduid als de-identificatie van de gegevens (de-identifying).
Het ingewikkelde aan datamasking is dat de gegevens na het toepassen van datamasking betekenisvol moeten blijven voor de toepassing (en het testen ervan).
Datamasking kent twee hoofdtypen:

- **Statische datamasking:** statische datamasking wordt toegepast op een kopie van de (gehele of gedeeltelijke) gegevensverzameling, waarna de kopie veilig kan worden verwerkt.
- **Dynamische datamasking:** bij dynamische datamasking wordt een gegeven gemaskeerd op het moment dat het gegeven worden doorgegeven of opgevraagd ("on-the-fly" ofwel "real time"). Welke gegevens wel of juist niet gemaskeerd worden kan afhankelijk gemaakt worden van de rechten van de gebruiker.

Datamasking maakt een veilige verwerking van persoonsgegevens mogelijk door het persoonsgegeven geheel of gedeeltelijk af te schermen.

7.5.5 Triple blind encryptie

De opslag van persoonsgegevens kan door de toepassing van 'triple blind' encryptietechnieken extra worden beveiligd in vergelijking tot standaard encryptie. Hierdoor worden de opgeslagen persoonsgegevens ook afgeschermd voor de partij die voor de opslag zorgt. Door de toepassing van 'triple blind' encryptietechnieken is niet alleen de opslag beveiligd, maar zijn de gegevens ook tijdens het opslaan zelf afgeschermd voor de partij die de gegevens beheert. Deze kan daarom de gegevens niet eenzijdig ontcijferen.
Triple blind encryptie kan ook worden toegepast voor de opslag van gegevens door de gebruiker zelf, bijvoorbeeld bij de opslag van gegevens op een token of mobiel apparaat. Triple blind encryptie schermt gegevens af voor de partij die de gegevens verwerkt.

7.5.6 Gegevens wiping

Wiping (schonen) van gegevens is het betrouwbaar verwijderen van gegevens van een opslagmedium, zoals harddisk of solid state geheugen, bijvoorbeeld in een mobiel device. Schonen van gegevens vindt plaats als het opslagmedium toegankelijk wordt voor anderen, veelal aan het eind van de gebruiksperiode.
Door schonen wordt toegang tot gegevens na de gebruiksperiode, dus na verwerking, voor andere verwerkingen voorkomen en waarmee (mis)gebruik van persoonsgegevens voor andere doelen, dan waarvoor ze zijn verzameld, wordt tegengegaan Dit vereenvoudigt de aantoonbaarheid van de doelbinding (U.01) en voorkomt misbruik door onbevoegden (U.04). Hoewel schonen in principe niet nodig is als alle data vercijferd is (en de toegang tot de sleutels is afgeschermd), vereenvoudigt het de aantoonbaarheid van de doelbinding en wordt de kans op kraken van de versleuteling voorkomen.

Wiping voorkomt dat gegevens achterblijven na de verwerking en gebruikt worden voor andere verwerkingen

7.5.7 Logging en monitoringsystemen

Loggingsystemen registeren dat toegang tot de informatie heeft plaatsgevonden. Het nakijken van de logging op verdachte handelingen, bijvoorbeeld het meermaals foutief authentiseren of het opvragen van persoons-gegevens afwijkend van het standaard gebruik, kan leiden tot aanvullend onderzoek. Actief monitoren van logging kan zelfs bijdragen aan het voorkomen van beveiligingsincidenten. Logging en monitoringsystemen

vormen daarmee een beschermingsinstrument in aanvulling op preventieve beveiligingssystemen. Voor de bescherming van zeer vertrouwelijke gegevens, zoals bijzondere persoonsgegevens, wordt alleen een preventief beveiligingssysteem - bij de huidige stand van de techniek - niet meer als afdoende gezien.

Bijzondere persoonsgegevens vragen om logging en monitoring als aanvulling op preventieve beveiligingssystemen

Logging en monitoring kan op verschillende niveaus plaatsvinden: van netwerkniveau tot applicatie- en databaseniveau. Logging op applicatieniveau heeft als voordeel dat logging en daarmee het vastleggen van afwijkingen door de applicatie effectief en efficiënt kan worden uitgevoerd.
Logging en monitoring systemen vormen naast een aanvulling op preventieve beveiligingssystemen ook een registratie die, bij lekken van persoonsgegevens, forensisch onderzoekers inzicht kan geven in de omvang, de oorzaak en daders van het datalek en vormt daarmee een belangrijk instrument in het kader van de Meldplicht Datalekken (C.03).

Loggingsystemen maken forensisch onderzoek mogelijk en vormen daarmee een belangrijk instrument in het kader van de Meldplicht Datalekken.

7.6 Technologieën voor een veilige doorgifte

7.6.1 Data loss prevention

Content-aware data loss prevention (DLP) is een techniek die real time ontdekt wanneer informatie (content) wordt doorgegeven of opgevraagd en kan filteren of blokkeren, afhankelijk van de context en het beleid. Dit wordt bij uitstek ingezet op de grenzen van een bedrijfsnetwerk en op dataservers met gevoelige informatie.

Data loss prevention vermindert risico's als onbedoeld of per toeval lekken van informatie of het ontsluiten van persoonsgegevens.

7.6.2 Cloud data protection gateways

"Cloud gegevensbescherming gateways" of "cloud encryptie gateways" zijn als gateway een tussenstation dat informatie versleutelt, waardoor opslag in de cloud door een dienstenleverancier veilig kan gebeuren. Deze technologie kan nuttig zijn als de opslag in een land plaatsvindt waar de privacy niet gewaarborgd is.
Als een dienstenleverancier de informatie moet kunnen verwerken in een applicatie, is veelal per gegevensveld ontcijfering door de gateway nodig. Deze oplossing beperkt daarmee het effectief functioneel gebruik van de gegevens door de applicatie.
Een bekende bewezen oplossing die de ontcijfering door een gateway in de cloud overneemt is gateway-software die op de cliënt/mobile device is geïnstalleerd. De verwerking van het persoonsgegeven en de afscherming door middel van encryptie gebeurt binnen één veilige omgeving, die zich geheel op de cliënt/mobile device bevindt.

Cloud gegevensbescherming gateways maken de opslag in niet vertrouwde omgevingen mogelijk en bieden de mogelijkheid van beperken van de persoonsgegevens die gedeeld worden.

7.6.3 E-mail encryptie

Het versturen van persoonsgegevens via email wordt niet meer als het gebruik van een voorziening met een passend beveiligingsniveau gezien. E-mail encryptie kan echter de vertrouwelijkheid en integriteit van het e-mail berichtenverkeer beschermen door het versleutelen van de e-mailberichten. Er bestaan verschillende standaarden [14] en oplossingen voor. Randvoorwaardelijk is dat het beheer van de sleutels bij een vertrouwde partij is ondergebracht. Vaak is DLP geïntegreerd in de e-mail encryptie oplossing.

Encryptie wordt als een minimum vereiste gezien voor het via e-mail versturen van persoonsgegevens.

8 Maatregelen voor het gebruik van mobiele apparaten

Tot nu toe is voornamelijk uitgegaan van de verwerking van persoonsgegevens in een veilige omgeving. Dus de verwerking op beveiligde kantoren en in beveiligde rekencentra. Wanneer echter persoonsgegevens worden verwerkt op een apparaat dat overal ingezet kan worden, dan zijn aanvullende maatregelen nodig om de verwerking daar veilig in te richten. Ook moet de afweging gemaakt worden of de verwerking in een onveilige omgeving überhaupt mogelijk of wenselijk is, zeker wanneer het bijzondere persoonsgegevens betreft. Apparaten die in niet-beveiligde omgevingen ingezet kunnen worden zijn laptops, smartphones, smart watches, smart cars, smart meters, etc. Eigenlijk alle apparaten waarop gegevens ontvangen en dus verwerkt kunnen worden buiten de genoemde veilige omgeving.
Dit hoofdstuk gaat in op de afwegingen en de te nemen maatregelen die nodig voor een veilige verwerking op mobiele apparaten. Ook wordt gekeken naar voorzieningen die eenieder kan inzetten voor het beschermen van de privacy op zijn of haar mobiele (privé-)apparaten.

8.1 Toegang tot de persoonsgegevens

De toegang tot persoonsgegevens moet, zoals beschreven is in paragraaf 7.2.2, altijd *rolgebaseerd* zijn, waarbij iedere verwerking past binnen de doelbinding en de taken die aan een bewerker zijn toegewezen. De bewerker is hij die het apparaat op dat moment in zijn bezit heeft, bedient en toegang heeft.

8.1.1 Context

Als gewerkt wordt op verschillende locaties, zoals locaties met interne (afgeschermde) werkplekken of locaties met externe (mogelijk niet-afgeschermde) werkplekken, dan is de locatie medebepalend voor hoe veilig het is persoonsgegevens te delen met deze werkplekken. Denk hierbij bijvoorbeeld aan dependances van de organisatie, de thuiswerkplek, de wifi-voorziening op terrassen of in hotels, wifi-hotspots en dergelijke. Ook tijdstip en de veiligheid van het mobiele apparaat kunnen meespelen in de afweging om persoonsgegevens te delen. De context (locatie, tijd en apparaat) is een belangrijke factor die absoluut moet worden meegewogen bij de afweging of het veilig en daarmee verantwoord is persoonsgegevens te delen met de bewerker die zich op dat moment in die context bevindt.
Binnen het RBAC-model wordt de toegang verzorgd op basis van rollen. Wanneer een veilig gebruik van de toegangsrechten ook bepaald wordt door de context (plaats, apparaat en tijd), dan schiet het RBAC-model te kort en moet het model uitgebreid worden met de Context. Hierdoor ontstaat het Rol en Context Based Access Model (RCBAC-model). De context is dan mede bepalend of de persoonsgegevens ingezien, veranderd of verwijderd mogen worden. Het meenemen van de context is zeker een vereiste wanneer toegang tot *bijzondere* persoonsgegevens wordt overwogen.

Bij de toegang vanaf werkplekken of mobiele apparaten met een verschillend beveiligingsniveau is naast de rol van een bewerker ook de context bepalend voor de keuze van de toegangsrechten.

8.1.2 Vertrouwelijkheid

De controle op de toegangsrechten in een bepaalde context kan verder worden uitgebreid door de controle op de vertrouwelijkheid van de gegevens. Dit kan op twee manieren plaatsvinden:

1. **Tagging**: De informatie wordt gemerkt om classificatie mogelijk te maken (Metadata Tags is een bekende methode);
2. **Scanning**: De informatie wordt gescand op bepaalde tekst bij het transporteren van de data.

Tagging (het toekennen van labels) kan zowel handmatig als geautomatiseerd gebeuren. Scanning gebeurt altijd geautomatiseerd. Handmatige tagging vereist veel discipline binnen een organisatie om alle informatie te voorzien van de juiste tags, dat wil zeggen de tags die de bijbehorende toepasselijke classificatie weergeven. Geautomatiseerde systemen (Rule Based Systems) zijn in opkomst, maar vereisen veel aandacht bij het initieel samenstellen van de Rule Base. Dit vereist kennis van de definitie van gevoelige informatie, waarbij deze definitie vaak afwijkt per organisatie: wanneer worden gegevens herkend als niet-vertrouwde gegevens, als persoonsgegevens of als bijzonder persoonsgegevens?

Een integrale classificatie en bijbehorende tags voor alle informatie die binnen een organisatie wordt verwerkt is doorgaans een lastige business case en dito implementatie. Vaak is het veel eenvoudiger om per systeem of per functionaliteit te bepalen of toegankelijk vanaf een externe (en daarmee minder vertrouwde) locatie wenselijk is.

De keuze voor de inzet van Tagging dan wel Scanning voor de afscherming van persoonsgegevens wordt gebaseerd op een businesscase.

8.2 Bescherming van gegevens op mobiele devices

Het risico van verlies of diefstal van mobiele devices is relatief groot en daarmee ook het gevaar dat persoonsgegevens in verkeerde handen kunnen vallen. Verschillende vergelijkbare oplossingen met encryptie en toegangscontrole beschermen de gegevens op mobiele devices. Doordat ze ingrijpen op het gehele device en daarmee in feite het hele gebruik beïnvloeden, zijn ze moeilijk(er) inzetbaar in organisaties die devices toestaan volgens het concept van "bring your own device" (BYOD). De eigenaar van het apparaat moet dan immers ingrijpend beheer vanuit de organisatie toestaan op zijn apparaat.

8.2.1 Mobile device management

Wanneer een organisatie zelf mobiele apparaten verstrekt en (verregaand) onder haar beheer houdt, dan is Mobile device management (MDM) of Enterprise Mobile Management (EMM) is een geschikte voorziening. Omdat de kennis over het veilig houden van het device bij de gebruiker in de praktijk veelal beperkt is, wordt het device als inherent onveilig gezien. Een voorziening als MDM zal hier voor de veiligheid moeten zorgen. Voorafgaand aan de toegang tot bijvoorbeeld een bedrijfsnetwerk kan gecontroleerd worden of MDM actief en up-to-date is. De maatregelen die door middel van MDM worden toegepast maken apps op een mobiel apparaat veilig voor communicatie met het organisatiedomein.
Als de app op het mobiele apparaat in de EMM of MDM omgeving draait, dan zorgen deze omgevingen voor een belangrijk deel ook voor de beveiliging van de verwerking van de persoonsgegevens in de app.
Doordat de instellingen door de EEM / MDM omgeving worden beheerd door of namens de organisatie die verantwoordelijk is voor de veilige verwerking, beperkt het gebruik van EMM /MDM zich tot apparaten die het eigendom zijn van de organisatie die verantwoordelijk is voor de verwerking.

MDM wordt als een minimum vereiste gezien
voor een veilige verwerking van persoonsgegevens op mobiele apparaten
door medewerkers van een organisatie.

8.2.2 Mobile Security Apps

Aanvullende apps voor de beveiliging van mobiele apparaten beschermen het apparaat, inclusief de prestaties, en ondersteunen de privacy. Typische kenmerken zijn antivirus scans, privacybeheer, optimalisatie van inrichting en prestaties, en diefstalbeveiliging. Ze zijn minder effectief in het beschermen van gebruikers tegen malware en dataverlies, omdat ze niet kunnen controleren wat gebruikers doen met hun apparaten (zoals "jailbreak" of "rooten" van het apparaat) en apps (zoals het downloaden van e-mailbijlagen). Doordat Mobile Security Apps alleen de beveiliging van het mobiele apparaat bewaken en niet de verwerking op het mobile apparaat afschermen, wordt steeds vaker getwijfeld aan de effectiviteit van Mobile Security Apps.

Mobile Security Apps kunnen de beveiliging van het mobiele apparaat bewaken.
De effectiviteit staat echter ter discussie.

8.2.3 Beveiligingseisen voor mobile apps

Het is voor organisaties een uitdaging om veilige apps te (laten) ontwikkelen. De methode "Grip op SSD" [10] geeft aan hoe de opdrachtgever sturing kan geven en verwachtingen kan expliciteren en de uitvoering kan bewaken. Een belangrijk onderdeel van de besturing met succes is het gebruik van een hanteerbaar(!) aantal beveiligingseisen. De SSDm(obile)-beveiligingseisen zijn een aanvulling op de SSD-beveiligingseisen voor applicaties op servers die in de methode "Grip op SSD" gebruikt worden om de verwachtingen tussen de

betrokken partijen te sturen. Ook als er sprake is van uitbesteding van ontwikkeling, onderhoud en aanbieden van de app in een app store. De beveiligingseisen houden rekening met de onderlinge verwachtingen tussen de betrokken partijen en benoemen daartoe de onderlinge verantwoordelijkheden om te kunnen voldoen aan de beveiligingseisen. Zie hiervoor SSDm, de SSD–eisen voor mobile apps [9].

Mobile Apps dienen een passend beveiligingsniveau te hebben. De SSD-eisen worden daarbij als minimum gezien.

8.3 Privacybescherming op Internet

Het waarborgen van de privacy op Internet vraagt om aanvullende maatregelen. In deze paragraaf wordt gekeken naar enkele voorzieningen die ingezet kunnen worden voor het beschermen van de privacy op en vanaf hun privé-apparaten op Internet.

8.3.1 EU Cookie Regels

Een cookie is een tekstbestandje op de computer van de websitebezoeker waarin door de website bepaalde gegevens worden opgeslagen. Websites moeten bezoekers informeren als zij cookies willen plaatsen. De bezoeker heeft dan de keuze over het wel of niet toestaan van de cookie(s). Ook het uitlezen van cookies die door andere websites zijn geplaatst mag alleen na goedkeuring van de bezoeker. Het doel van deze Cookiewet is om de privacy van de gebruiker beter te beschermen. De bezoeker moet daarvoor toestemming geven. Dat geldt strikt genomen alleen voor cookies die surfgedrag bijhouden. De regels voor cookies staan art. 11.7a van de Telecommunicatiewet (Tw), de zogenoemde cookiebepaling. De wet is een implementatie van de Europese ePrivacy Richtlijn 2002/58/EC. De regels verschillen per soort cookie [13].

- **Functionele cookies (zijn uitgezonderd):**

  Websites hebben geen toestemming nodig voor het plaatsen van functionele cookies die nodig zijn om een dienst of webshop te laten functioneren. Dit zijn bijvoorbeeld bestanden die bijhouden wat er in een digitaal winkelwagentje zit.

- **Analytische cookies (wordt versoepeld):**

  Op dit moment moeten websites ook voor analytische cookies toestemming vragen. De minister van Economische Zaken wil het verplicht vragen van toestemming voor analytische cookies afschaffen. Websites gebruiken analytische cookies om bezoekersaantallen bij te houden. Ze hebben nauwelijks gevolgen voor de privacy. Wel zorgen ze vaak voor pop-ups waarin om toestemming wordt gevraagd.
  Door de geplande versoepeling hoeft een website alleen om toestemming te vragen als dit ook echt nodig is om de privacy te beschermen. Dat kan ook bij analytische cookies in sommige gevallen nodig zijn. Bijvoorbeeld wanneer de verzamelde statistische gegevens ook worden gebruikt voor het opbouwen van bezoekersprofielen.

- **Tracking cookies (altijd toestemming vereist):**

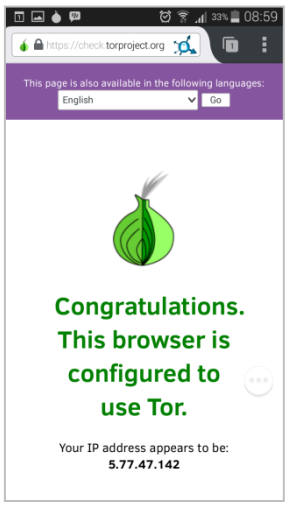
  Bij het plaatsen van zogenaamde 'tracking cookies' moet een website de bezoeker altijd informeren en om toestemming vragen. Tracking cookies worden gebruikt om individueel surfgedrag bij te houden en om profielen op te stellen. Naast de Telecommunicatiewet is ook de Wet bescherming persoonsgegevens op deze cookies van toepassing.

Mogelijk omdat het algemeen als onduidelijk wordt ervaren hoe cookies in browsers ingesteld moeten worden, zijn er veel overtredingen van deze wetgeving. Wel hebben de meeste websites een oplossing gevonden die werkt voor hen (goed zichtbaar vragen om toestemming). Een ander effect van deze wetgeving is dat gebruikers al snel 'klikmoe' zijn of weten dat ze niet echt een keuze hebben en daardoor standaard accepteren. Een mogelijke oorzaak ligt in de keuze van bouwers van websites die niet privacy by default als principe te hanteren.

De EU Cookie regels worden als hinderlijk ervaren. Door privacy by default als principe te hanteren kan voorkomen worden dat gebruikers 'klikmoe' worden.

8.3.2 Communication Anonymizers

Communication Anonymizers verbergen de echte online identiteit (e-mailadres, IP-adres, enz.) en vervangen deze door een niet-traceerbare identiteit. Dit is een meer geavanceerde aanpak om te voorkomen dat de identiteit van een gebruiker te achterhalen is, dan de zogenoemde "gedeelde nep-accounts". Hierbij creëert een persoon een account met valse gegevens en deelt vervolgens het user-id en wachtwoord op Internet. De locatie van de gebruiker is niettemin, door middel van het IP-adres, toch te achterhalen. Hierdoor is de 'anonimiteit' bij het gebruik van deze nep-accounts beperkt. De nauwkeurigheid van de locatie is afhankelijk van informatie van de provider via welke de gebruiker toegang heeft tot Internet.



Een belangrijke voorziening voor anonieme communicatie is het TOR-netwerk. Het TOR-project biedt vrij verkrijgbare software voor het inschakelen van de anonieme communicatie. TOR leidt het Internetverkeer via een gratis, wereldwijd netwerk van vele routeringspunten, waardoor de gebruiker in een handomdraai beschikt over steeds een wisselend IP-adres, waarmee hij zich op het Internet vertoont. De werkelijke locatie van een gebruiker wordt daardoor moeilijk te achterhalen. Het wordt ook gebruikt om Internetblokkades, ingesteld door de overheden in landen met censuur, te omzeilen.
Bedenk wel dat anonimisering indruist tegen het gangbare businessmodel van de Internetbedrijven en overheden. Het is een kat-en-muis spel, waarbij je op geen enkel moment zeker kunt zijn van anonimiteit. Ook TOR is in dit opzicht aan erosie onderhevig.

TOR netwerken maken het moeilijk te achterhalen waar de gebruiker zich op het Internet bevindt.
Anonimiteit is echter niet 100% te garanderen

8.3.3 Privacy Controlled Sociale Netwerken

Een privacy-gecontroleerd sociale netwerk (PCSN) is een openbaar toegankelijke sociale netwerkdienst, waarbij privacy meer aandacht krijgt in vergelijking met veel bestaande sociale media platformen die bijvoorbeeld afhankelijk zijn van het genereren van inkomsten uit context-aware reclames.
Zij doen dat onder andere door:

- Sterke controle van de privacy van de communicatie en de inhoud op het sociale platform;
- De gebruiker heeft controle over de levenscyclus van gedeelde grafische en tekstuele inhoud;
- Verificatie van de identiteit van leden van het sociale netwerk;
- Privacy (beter) contractueel geregeld.

Privacy Controlled Sociale Netwerken kunnen voorkomen dat persoonsgegevens worden uitgewisseld via niet veilige sociale netwerken.

Referenties

[1] Privacy by Design. *Strong Privacy Protection – Now, and Well into the Future*. A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners (2011); https://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=1125 ; https://www.ipc.on.ca/images/Resources/PbDReport.pdf; www.privacybydesign.ca
[2] Privacy: van organisatorisch beleid naar Privacy Enhancing Technologies; Drs. ing. R.F. Koorn CISA RE en drs. J. ter Hart; Compact 2004/3
[3] Beleid Granulariteit, Ir. M.G.J. Koers; 1 maart 2006; UWV
[4] Testen op ACID-eisen; UWV; 2004; zie Bijlage 1: Testen op ACID-eisen
[5] Grip op beveiliging in inkoopcontracten; CIP; oktober 2014; http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-Beveiligingsovereenkomsten-v1_0.pdf
[6] Handreiking Beveiligingsbeleid Clouddiensten; april 2014; http://www.cip-overheid.nl/wp-content/uploads/2014/04/Beveiligingsbeleid-clouddiensten-CIP-DEF-v2_3-excl-ARD.pdf
[7] https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf; geraadpleegd op 10 januari 2014
[8] Testen met persoonsgegevens; oktober 2013; http://www.cip-overheid.nl/downloads/testen-met-persoonsgegevens/
[9] Grip op SSD: beveiligingseisen voor mobile apps; 15 oktober 2015; http://www.cip-overheid.nl/downloads/grip-op-ssd/
[10] Grip op SSD: beveiligingseisen voor (web-)applicaties; versie 2.0; 5 oktober 2014; http://www.cip-overheid.nl/downloads/grip-op-ssd/
[11] http://www.nationaalarchief.nl/waardering-selectie/selectielijsten
[12] http://www.cip-overheid.nl/downloads/beveiligingsbeleid-clouddiensten/
[13] http://www.rijksoverheid.nl/onderwerpen/Internet/bescherming-privacy-op-Internet/cookiewet-regels-en-richtlijnen
[14] http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

Bijlage 1: Testen op ACID-eisen

Onderwerp : Aantonen van Failover en voldoen aan ACID-principes
Datum : UWV 27 mei 2004

ACID-testen
Om achterhalen of in voldoende mate aan de ACID-principes wordt voldaan zullen de volgende testen in runtime uitgevoerd moeten worden:

Toestand : Een gepauzeerde transactie		
1	Concurrency - Uncommited Read test	Via een aparte sessie wordt een select query uitgevoerd op de waarde die reeds in de database gemuteerd is, maar nog niet is gecommit.
	Verwacht resultaat	De niet-gecommitte waarde mag niet worden getoond.
2	Concurrency - Repeatable Read test	Via een aparte sessie wordt een update-query afgevuurd op een rij waarop een referentiele controle is uitgevoerd, maar die nog niet is gecommit.
	Verwacht resultaat	De gecontroleerde waarde mag niet worden gewijzigd zolang de transactie van de pauzerende actie nog steeds actief is.
Toestand : na succesvolle afronding van de gepauzeerde transactie		
3	Durable database test	Er wordt een select-query uitgevoerd op de waarden die naar de database zijn weggeschreven.
	Verwacht resultaat	Alle geselecteerde waarden worden als antwoord terug gegeven.
4	Durable queue test	Het verwerkte bericht wordt in de queue opgevraagd.
	Verwacht resultaat	De opvraag levert geen bericht op.
Toestand : na afbreken van de gepauzeerde transactie		
5	Atomic database test	Er wordt een select-query uitgevoerd op de waarden die naar de database zijn weggeschreven.
	Verwacht resultaat	De geselecteerde waarden worden als antwoord terug gegeven.
6	Atomic queue test	Het niet-verwerkte bericht wordt in de queue opgevraagd.
	Verwacht resultaat	De opvraag levert wel een bericht op