*H.J.M. Joosten**

Aantoonbaar voldoen aan (komende) privacy- wet- en regelgeving in een IT-rijke context

93

Trefwoorden:
wettelijke compliance, wetten formaliseren, geautomatiseerde ondersteuning, traceerbaarheid, Ampersand, privacyassistent

De Europese Commissie heeft in januari 2012 een nieuwe richtlijn en verordening voorgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens [1, 2]. Deze zijn bedoeld om de huidige Data Protection Directive 95/46/EC te vervangen. Als de verordening wordt aangenomen moet niet alleen compliance kunnen worden aangetoond maar kunnen straffen voor overtredingen voor organisaties oplopen tot 2% van hun jaarlijkse wereldwijde omzet. Compliance aantonen is op zichzelf al moeilijk en wordt nog lastiger naarmate de complexiteit van (geautomatiseerde) informatieverwerkingen toeneemt en/of deze verwerkingen voor andere (nieuwe) doeleinden worden gebruikt ('function creep'). Dat dit gebeurt is onontkoombaar – het is immers onderdeel van veel innovaties. In dit artikel verkennen we de (on)mogelijkheden om te komen tot een 'privacyassistent': een systeem dat organisaties ondersteunt bij het compliant worden en compliant blijven, ook in situaties waarin wordt geïnnoveerd en persoonsgegevens voor nieuwe doeleinden worden gebruikt.

1 Inleiding

Berichten over het schenden van privacy in de digitale wereld komen zo veelvuldig voor, dat alleen nog de allergrootste opvallen, zoals een incident waarbij callcentermedewerkers van het grootste commerciële verzuimbedrijf van ons land zonder een medische opleiding, medische vragen stellen aan zieke werknemers [3]. Niet lang daarna bleek dat ook de software die hierbij werd gebruikt toeliet dat medische en persoonsgegevens van meer dan 300 000 werknemers maandenlang toegankelijk waren voor onbevoegden [4].

De hoeveelheid en variëteit in privacyincidenten is erg groot. WebWereld had oktober (2011) uitgeroepen tot 'Lektober: maand van het privacylek' en elke werkdag een nieuw lek gepubliceerd [5]. Recentere nieuwsberichten gaan onder meer over populaire Android-apps die gevoelige gegevens stelen [6], het CBP dat vaststelde dat Albert Heijn de Wet bescherming persoonsgegevens (Wbp) overtrad met haar nieuwe voordeelprogramma rond de bonuskaart [7], het CBP dat een dwangsom van € 125 000 inde van de NS voor het bewaren van persoonsgegevens na de maximale bewaartermijn [8], of de KLPD die slecht beveiligde spyware (van de Duitse politie) inzette die zich gemakkelijk liet manipuleren [9].

Een belangrijke oorzaak voor privacyincidenten is 'function creep': het (her)gebruiken van gegevens voor andere doeleinden dan die waarvoor ze zijn verzameld. Zo was het burgerservicenummer oorspronkelijk alleen bedoeld om contacten tussen burgers en de overheid te onderhouden. Inmiddels wordt het ook binnen de zorg gebruikt en binnenkort wellicht in de financiële sector [10]. Een ander voorbeeld zijn de camera's die nummerplaten kunnen herkennen [11]. Partijen (zoals politie, KMar, gemeenten, inspectie V&W, belastingdienst/douane, stichting CrimiNee!) hebben die weliswaar opgehangen voor hun eigen doeleinden, maar ze zijn potentieel ook bruikbaar voor doeleinden van een ander. Voor opsporing zijn beelden van camera's van Rijkswaterstaat of van de gemeentelijke Dienst Stedenbouw en Volkshuisvesting van Rotterdam ook bruikbaar. Waarom zou je zelf systemen in stand houden en beheren als je gebruik kunt maken van iets anders dat er al is? Hergebruik is een belangrijke pijler voor innovaties, maar kan gemakkelijk op gespannen voet komen te staan met het in de Wbp neergelegde beginsel van doelbinding [12].

Dit dilemma wordt steeds belangrijker omdat (IT-)
diensten steeds vaker worden hergebruikt en function creep dus steeds vaker aan de orde is. Dat dit steeds meer gebeurt, zien we niet alleen in de operationele praktijk – organisaties besteden steeds meer uit [13] – maar ook in de ontwerppraktijk waar 'hergebruik' expliciet als ontwerp- of architectuurprincipe wordt benoemd [14]. Naarmate hergebruik toeneemt zullen schakels die in de traditioneel lineaire dienstenketens (silo's) steeds één voorganger en één opvolger hebben, veranderen in netwerkknooppunten met arbitrair veel voorgangers en opvolgers. Maar als elk knooppunt met steeds meer en verschillende knooppunten gaat samenwerken, wordt het steeds ingewikkelder om per knooppunt overzicht te houden over welke verwerkingen op welke gegevens mogen plaatsvinden en welke doelen dat dan dient. Het feit dat we een steeds meer genetwerkte samenleving worden, maakt het dus enerzijds moeilijker om te besluiten of een gegevensverwerking wel plaats mag vinden

* **Rieks Joosten (rieks.joosten@tno.nl) is werkzaam als onderzoeker bij TNO op het gebied van informatiebeveiliging. Zijn bijzondere aandacht gaat uit naar de integriteit van bedrijfsprocessen, risicomanagement, identity- en accessmanagement en het specificeren/ontwerpen van geautomatiseerde ondersteuning hiervoor.**

en anderzijds gemakkelijker – bijvoorbeeld door standaardisatie – om gegevens te delen en te verwerken. Hierdoor komt compliance aan de Wbp in het gedrang en kan de aantoonbare compliance zoals die in het EU-voorstel wordt geëist, een groot probleem worden.

Een tweede trend is de toenemende hoeveelheid aan 'open data' die geacht wordt grote economische voordelen met zich mee te brengen. Gegevens zoals de gemiddelde koopsom van huizen in de buurt van een locatie, die op zich geen persoonsgegevens zijn, kunnen dat – in combinatie met andere gegevens – toch worden. Door technologische innovaties en de toename van de hoeveelheid 'open data' kunnen gegevens die op dit moment geen persoonsgegevens zijn, dat volgend jaar wellicht wel zijn. Dat maakt het in toenemende mate moeilijk om aan de privacywetgeving te (blijven) voldoen [15]. Nog niet zo lang geleden waren IP-adressen, woonadressen, telefoonnummers en dergelijke nog geen persoonsgegevens. Dat zijn ze inmiddels wel.

Een derde trend is het groeiende aantal individuen en mkb'ers dat software maakt of gebruikt. Zij zijn te klein om alles te kunnen weten en het kan ze dan ook gemakkelijk ontgaan dat ze privacyverplichtingen hebben c.q. welke dat zijn. Illustratief hiervoor is de tekst die naar aanleiding van het incident met VerzuimReductie en VCD [3, 4] verscheen op LinkedIn: 'Huisartsvandaag.nl meldt dat volgens het CBP een datalek in het EPD straks ook de verantwoordelijkheid is van de huisarts. Kan je een hulpverlener in de eerste lijn verantwoordelijk stellen voor datalekken en kan je verwachten dat de hulpverlener controleert of zijn/haar softwareleverancier voldoet aan de toetsbare eisen van de NEN 7510?'.[1]

2 Wettelijke compliance

Aantoonbaar naleven van de Wbp of andere privacywetten houdt uiteindelijk in dat men zich voor een toezichthouder c.q. rechter moet kunnen verantwoorden. Dat is niet hetzelfde als de wet tot de letter naleven. Het gaat eerder om het kunnen innemen van een juridisch verdedigbare positie mocht het tot een rechtszaak komen [16]. 'Due diligence' volstaat, dat wil zeggen dat binnen de grenzen van het redelijke alle moeite is gedaan om zich ervan te vergewissen dat aan de wettelijke vereisten is voldaan [17].

Om dit te kunnen is in de eerste plaats nodig dat binnen de grenzen van het redelijke alle moeite wordt gedaan om de wet goed te interpreteren. Dit is niet triviaal, omdat de wetgever enerzijds duidelijke regels moet stellen maar anderzijds rekening moet houden met maatschappelijke en technologische veranderingen die zich ongetwijfeld voor zullen gaan doen [18]. Het gevolg hiervan is dat wetten vaag kunnen zijn, gebruik kunnen maken van evaluatieve termen en een open structuur hebben [19]. Een voorbeeld hiervan is de term 'verwerking', die gedefinieerd wordt als 'handeling of geheel van handelingen' (artikel 1 sub b Wbp) c.q. 'bewerking of geheel van bewerkingen' (artikel 4 lid 3 Algemene verordening gegevensbescherming (AVG) [2]). Dit kan niet alleen feitelijk uitgevoerde handelingen (feitelijke verwerkingen) betekenen, maar ook mogelijk uit te voeren handelingen (soorten handelingen, of potentiële verwerkingen). Artikel 4 lid 5 AVG stelt dat de 'voor de verwerking verantwoordelijke […] het doel van en de voorwaarden en middelen voor de verwerking van persoonsgegevens vaststelt'. Het gaat hier duidelijk om potentiële (soorten) verwerkingen, omdat feitelijke handelingen niet eerder uitgevoerd kunnen worden dan dat doel, voorwaarden en middelen zijn vastgesteld. In artikel 5 onder f AVG, die stelt dat de voor de verwerking verantwoordelijke […] ervoor zorgt en aantoont dat elke verwerking voldoet aan de bepalingen van deze verordening, lijkt echter de feitelijke verwerking te zijn bedoeld.

In de tweede plaats is nodig dat we binnen de grenzen van het redelijke alle moeite doen om vast te stellen hoe de praktische realiteit is gerelateerd aan de wettelijke terminologie. Stel dat een zekere computer persoonsgegevens op een zekere manier bewerkt en als verwerkingsmiddel wordt (her)gebruikt voor verschillende potentiële verwerkingen, elk met verschillende verantwoordelijken en doelen. Om vast te kunnen stellen wie voor die feitelijke verwerking verantwoordelijk is, en ten behoeve van welk(e) doel(en) die feitelijke verwerking heeft plaatsgevonden, is het noodzakelijk dat de feitelijke verwerkingen consequent van potentiële kunnen worden onderscheiden.

Het hebben en houden van een (voldoende) compleet, courant, consistent en coherent overzicht over zulke verwerkingen (alsmede de bijbehorende organisaties, processen en systemen) is nodig om (binnen de grenzen van het redelijke) compliance aan te kunnen tonen. Menselijke begrenzingen van onder meer fysiologische en linguïstische aard belemmeren ons echter in het maken en beheren ervan [20, 21]. De Wetenschappelijke Raad voor het Regeringsbeleid constateert dat ook en zegt dat het menselijkerwijs vrijwel onmogelijk is om een kloppend overzicht te krijgen, laat staan actueel te houden, van de verschillende verwerkingen binnen de overheid [12]. Ze wijzen dan niet alleen op de grote hoeveelheid aan organisaties, processen en systemen, maar ook op de veranderlijkheid ervan 'vanwege nieuwe technologische mogelijkheden, politiek-bestuurlijke ambities en wensen en verwachtingen in de samenleving'.

Om wettelijke compliance voor genetwerkte systemen aantoonbaar te maken is geautomatiseerde ondersteuning noodzakelijk, zelfs als het om schijnbaar 'eenvoudige' systemen gaat. Een voorbeeld daarvan is het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT), een soort geautomatiseerd 'doorgeefluik' waar aanbieders van openbare telecommunicatienetwerken en -diensten, gebruikers- en verkeersgegevens leveren die veiligheids- en opsporingsinstanties kunnen afnemen ten behoeve van opsporing. Wat wel en niet mag c.q.

1 www.linkedin.com/groupItem?view=&gid=119463&type=member&item=110257528&qid=4ce08d30-533b-4cb7-b740-1e7fbbcd7307&trk=group_search_item_list-0-b-ttl.

moet is geregeld in het 'Besluit verstrekking gegevens telecommunicatie' (Bvgt). De Inspectie Veiligheid en Justitie heeft onderzoek gedaan naar de rechtmatigheid van de bevragingen die politiekorpsen doen aan het CIOT en vastgesteld dat de administratieve last om 'compliance' aan het Bvgt aan te tonen erg groot is en audits niet efficiënt zijn uit te voeren, wat het toezicht bemoeilijkt [22]. Ook hebben zij vastgesteld dat daar waar geautomatiseerde ondersteuning wordt gebruikt, deze problemen niet spelen, en adviseren daarom om voor dit soort bevragingen een geautomatiseerd ondersteuningssysteem te implementeren dat direct alle relevante documenten voor het vaststellen van de rechtmatigheid van bevragingen vastlegt en toezicht hierop vereenvoudigt [22].

3 Geautomatiseerde ondersteuning

Computers kunnen mensen op een aantal punten ondersteunen. Zo kunnen computers veel meer gegevens opslaan en aan elkaar relateren, dan mensen dat doen. Voor het CIOT-systeem hebben we het bijvoorbeeld over gegevens van 2,3 miljoen bevragingen (2011, exclusief bevragingen door de AIVD en MIVD) die aan het Bvgt moeten voldoen [22].

In de tweede plaats kunnen computers ondersteunen door te signaleren waar zich onvolledigheden in de gegevenshuishouding voordoen, waardoor toetsen op compliance niet kunnen worden uitgevoerd. Als bijvoorbeeld van een verwerking niet is geregistreerd wie ervoor verantwoordelijk is/zijn, of als niet is gespecificeerd voor welke doelen persoonsgegevens worden verzameld c.q. verwerkt, dan zijn signalen hieromtrent hulpmiddelen die het mogelijk maken de informatie te completeren.

In de derde plaats kunnen ze inconsistenties in de gegevenshuishouding constateren waardoor toetsen op compliance mogelijk de verkeerde uitkomsten opleveren. Om compliance aan artikel 12 lid 1 Wbp aan te tonen voor een transactie waar persoonsgegevens bij betrokken zijn, moet worden vastgesteld dat degene die persoonsgegevens bewerkt hiertoe een wettelijke plicht heeft of dit doet in opdracht van een verantwoordelijke met wie hij (met betrekking tot dit type transacties) een relatie heeft. Daartoe is het nodig dat van de verschillende soorten gegevenstransacties wordt geregistreerd of daarvoor wettelijke verplichtingen bestaan voor de bewerker (en zo ja, welke dat dan zijn). Ook is nodig te registreren welke relatie(s) bewerkers en verantwoordelijken hebben ten aanzien van welk type gegevenstransacties. Met deze informatie kunnen computers toetsen of aan artikel 12 lid 1 Wbp is voldaan dan wel signaleren dat dit niet kan worden vastgesteld.

Het signaleren van onvolledigheden en inconsistenties kan een computer alleen op basis van geformaliseerde regels die een adequate afbeelding zijn van de betreffende wetsartikelen. Dat dit niet triviaal is laten we zien aan de hand van artikel 9 Wbp. Het eerste lid zegt: 'Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen'. Het tweede lid zegt dat een dergelijk besluit toekomt aan de verantwoordelijke en dat daarbij in ieder geval met een vijftal overwegingen rekening moet worden gehouden. Het derde lid specificeert een aantal gevallen waarin persoonsgegevens mogen worden verwerkt ondanks dat ze zijn verzameld voor andere doeleinden dan waarvoor ze worden verwerkt. Compliance aan artikel 9 Wbp kan dus niet altijd automatisch worden vastgesteld, vaak moet eerst een aantal menselijke besluiten zijn genomen betreffende die verwerking. Computers kunnen wel nagaan of er (en welke) besluiten zijn geregistreerd waarin staat welke doelen met welke (andere) doelen verenigbaar zijn voor een zekere verantwoordelijke. Als van gegevens de verzameldoelen zijn geregistreerd en van elke soort transactie de doelen bekend zijn, dan kan een computer van een willekeurige gegevenstransactie vaststellen of de doelen waarvoor de bij de transactie betrokken persoonsgegevens waren verzameld, volgens de voor de transactie verantwoordelijke partij verenigbaar zijn met de doelen van de transactie zelf. Als de computer een transactie signaleert waarvoor dit niet kan worden vastgesteld, dan is de verantwoordelijke in overtreding van artikel 9 Wbp, of is de registratie van besluiten niet up-to-date. Ongeacht de oorzaak van het signaal moet de verantwoordelijke actie ondernemen, hetzij om weer te gaan voldoen aan artikel 9 Wbp, hetzij om de aantoonbaarheid te verbeteren.

Om de juiste ondersteuning te bieden bij het vaststellen van compliance, moeten computers over een actuele, aan de wet ontleende, geformaliseerde regelverzameling beschikken, vooral als die wet (frequent) wijzigt. Dat dit met traditionele automatisering problemen oplevert heeft de IND in 2004 aan den lijve ervaren [23, 24]. Het vernieuwende idee van het INDiGO-programma bestond uit het scheiden van de 'know' (wettelijke regels) en de 'flow' (de procesgang) [25]. De processen blijven immers steeds hetzelfde (op elke aanvraag voor een verblijfsvergunning moet immers steeds een besluit genomen worden of de vergunning wordt verleend), maar de regels op basis waarvan de processen werken (besluiten genomen worden), kunnen (frequent) veranderen. De IND heeft hiermee de NAF-architectuurprijs 2009 gewonnen [26]. Vanuit de automatisering gezien is het dus mogelijk om geautomatiseerde ondersteuning te bouwen voor processen die aan de wet moeten voldoen, waarbij de wetsartikelen zelf als regels in het systeem worden gebracht. Overigens spreekt dit allerminst vanzelf: ook INDiGO kent nog steeds problemen. Dat ligt echter niet aan het idee of de IT, maar aan het beheer en de afstemming met de beheersorganisatie [27, 28].

We constateren dat het mogelijk is om de in deze wetten en regels benoemde entiteiten (zoals 'verantwoordelijke', 'verwerking', 'verwerkingsdoel' e.d.), hun onderlinge relaties en samenhangen (regels) te formaliseren. Daarmee kunnen we geautomatiseerde ondersteuning bouwen wiens taak het is om ontbrekende informatie, ondeugdelijke samenhangen en 'overtredingen' van geformaliseerde wet- en regelgeving te signaleren. Het 'wegwerken' van deze signalen leidt tot betere compliance aan de betreffende wet- en regelgeving. Het effect van wetswijzigingen is relatief overzichtelijk: door deze

veranderingen door te voeren in de verzameling van geformaliseerde regels zal het systeem andere signalen afgeven, overeenkomend met de wijzigingen in de wet.

Om te bewijzen dat 100% aan de wet is voldaan moet echter eerst worden vastgesteld dat de geformaliseerde regelverzameling deze wet voor 100% afdekt. Dat lijkt echter niet nodig als kan worden aangetoond dat binnen de grenzen van het redelijke alle moeite is gedaan om de wet goed te interpreteren en tot een goede formalisering te komen.

4 Compliance, traceerbaarheid, 'Ampersand' en ADL

Om (zo veel mogelijk) geautomatiseerd vast te kunnen stellen of in een zekere context aan een zekere verzameling regels (wetsartikelen) is voldaan, moeten we elke regel uit die verzameling 'formaliseren', d.w.z. een formulering voor die regel opstellen die op zichzelf voldoende is om computers te laten vaststellen of (binnen een gegevensverzameling) al dan niet aan de regel is voldaan. Een dergelijke 'formele regel' moet (binnen de context) eenduidig zijn en consistent met de andere regels. Ook moet er een computerprogramma (compiler) bestaan die dergelijke formele regels kan omzetten in voor de computer uitvoerbare code.

Uitdrukkingen van regels in een natuurlijke taal voldoen hier in het algemeen niet aan. Er bestaat immers geen compiler (vertaler) die natuurlijke taal kan omzetten in een computerprogramma. Uitdrukkingen in een bekende computertaal (zoals 'C', 'PHP', 'Java') voldoen in principe wel, maar zijn niet vanzelfsprekend eenduidig omdat de compilers die programmateksten omzetten in executeerbare code dit op verschillende manieren doen en de instructies die een computer moet uitvoeren dus afhangen van welke vertaler werd gebruikt. Talen die gebruikt worden in wiskundige disciplines als predicatenlogica of relatie algebra, voldoen wel, hoewel compilers hiervoor erg schaars zijn.

Ampersand is een nieuwe methode voor het extraheren en formeel beschrijven van regels c.q. vereisten die, impliciet of expliciet, uitgedrukt zijn in een of andere natuurlijke taal, zoals wetteksten [29]. Het nut hiervan is dat uit de formele beschrijving systemen kunnen worden gegenereerd.

Een dergelijk systeem kan van gegevensverzamelingen signaleren in hoeverre ze de geformaliseerde regels overtreden. Als bijvoorbeeld een database gegevens zou bevatten van de 2,3 miljoen bevragingen van het CIOT-systeem, dan zou een systeem dat vanuit de betreffende wet- en regelgeving zou zijn gegenereerd, alle overtredingen van die wet- en regelgeving signaleren.

Een dergelijk systeem zou ook procesondersteuning kunnen bieden, bestaande uit het voorkómen dat deze regels worden overtreden. Een voorbeeld is de procesondersteuning voor het aanvragen en uitgeven van de Verklaring omtrent het gedrag (VOG), waarbij dat deel van de Wet c.q. het Besluit op de justitiële en strafvorderlijke gegevens is geformaliseerd dat betrekking heeft op de VOG [30].

Elk signaal of ingrijpen kan overigens worden getraceerd naar de bronteksten (zoals wetsartikelen) waarop dat signaal of ingrijpen wordt gebaseerd. De taal die Ampersand gebruikt voor het formeel beschrijven van regels en het traceerbaar houden hiervan naar de bronteksten, heet ADL.

ADL voorziet in de mogelijkheid om verschillende uitdrukkingsvormen (in verschillende talen) van één enkele regel aan elkaar te relateren. Zo kan een regel die vervat is in een wetsartikel worden opgeschreven in natuurlijke taal (de tekst van het wetsartikel en/of een verwijzing daarheen) en ook in de notatie die bij relatie algebra[2] gebruikelijk is. Ook definities van verschillende concepten, zoals 'verwerking', 'verantwoordelijke' e.d., kunnen enerzijds worden beschreven in natuurlijke taal (ontleend aan de wetteksten) en anderzijds als objecttype in relatie algebra.

Figuur 1 toont hoe voor verwerkingen verantwoordelijke (partijen) in ADL worden uitgedrukt.

De bovenste regel in de figuur definieert de relatie in relatie algebra. De volgende regel (die met 'PRAGMA' begint) specificeert de overeenkomstige natuurlijke taal zin: 'Voor 'verwerking' draagt 'partij' (me)de verantwoordelijkheid in de zin van de Wbp'. Vervolgens wordt gedocumenteerd wat het bestaan van deze relatie rechtvaardigt. In dit geval zijn dat twee wetsartikelen. Op deze manier wordt de relatie 'verwerkingsVerantwoordelijke' traceerbaar naar de gebruikte bron(nen).

```
verwerkingsVerantwoordelijke :: Verwerking * Partij
PRAGMA "Voor " " draagt " " (me)de verantwoordelijkheid in de zin van de Wbp"
PURPOSE RELATION verwerkingsVerantwoordelijke REF "Artikel 1 sub d Wbp"
{+In de Wbp en de daarop berustende bepalingen wordt verstaan onder VERANTWOORDELIJKE: de
natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen
of te zamen met anderen, het doel van en de middelen voor de VERWERKING vaststelt.-}
PURPOSE RELATION verwerkingsVerantwoordelijke REF "Artikel 28 sub a Wbp"
{+Een melding van een (geheel of gedeeltelijk geautomatiseerde VERWERKING) als bedoeld in
Artikel 27 eerste lid, behelst een opgave van de naam en het adres van de
VERANTWOORDELIJKE.-}
```

Figuur 1. Voorbeeld van de specificatie van een relatie in ADL die rechtstreeks ontleend wordt aan de Wbp

2 Voor het formeel uitdrukken van regels gebruikt Ampersand relatie-algebra, een (150 jaar) oude en goed begrepen wiskundige discipline. Voor de leesbaarheid is de formele regel hier als leesbare tekst opgeschreven.

```
svcVerwerkingsDoel :: Service * Doel
PRAGMA "" " verwerkt gegevens ten behoeve van "
PURPOSE RELATION svcVerwerkingsDoel REF "Artikel 11 eerste lid Wbp"
{+PERSOONSGEGEVENs worden slechts verwerkt voor zover zij, gelet op de doeleinden
waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend
en niet bovenmatig zijn. Daarom moet van elke service die persoonsgegevens verwerkt
bekend zijn ten behoeve van welk(e) doel(en) die verwerking plaatsvindt.-}
PURPOSE RELATION svcVerwerkingsDoel REF "Artikel 28 sub b Wbp"
{+Een melding van een (geheel of gedeeltelijk geautomatiseerde VERWERKING) als bedoeld in
Artikel 27 eerste lid, behelst een opgave van het doel of de doeleinden van de svc.-}
```

Figuur 2. Voorbeeld van de specificatie van een relatie die indirect uit de Wbp wordt gemotiveerd

Naast concepten en regels die rechtstreeks aan de wet kunnen worden ontleend, willen we ook concepten en regels gebruiken waarmee processen, applicaties, services, systemen enzovoorts kunnen worden gemodelleerd zoals die in ontwerpdocumenten worden gebruikt. Dan immers kunnen we het uitwisselen van gegevens tussen computers formeel beschrijven en een formele regel opschrijven waarmee kan worden vastgesteld of een zeker type gegevensuitwisseling al dan niet voldoet aan de wettelijke eisen. Figuur 2 geeft hiervan een voorbeeld.

Met de formele gespecificeerde concepten en relaties kunnen we hiermee ook regels formaliseren. Figuur 3 geeft hiervan een voorbeeld.

Na 'RULE' volgt de naam van de regel. De volgende regel bevat de regel in termen van relatie algebra. Daarna (achter 'MEANING') volgt de regel in natuurlijke taal – deze is weer ontleend aan de wet. Achter 'VIOLATION' wordt de tekst gespecificeerd die gebruikt wordt om te signaleren als niet aan de regel wordt voldaan. Als bijvoorbeeld een persoonsgegeven 'naam' bestaat maar er is geen verzameldoel van bekend, dan wordt dit gesignaleerd door de tekst 'Van persoonsgegeven "naam" is geen doel bekend waartoe het is verzameld'. Daarna volgt de motivatie van het bestaansrecht van deze regel, waarbij naar artikel 7 Wbp wordt verwezen.

ADL biedt ook de mogelijkheid om voor verschillende rollen (zoals die van verwerker, bewerker, derde, betrokkene, privacyfunctionaris enz.) gebruikersinterfaces te definiëren die geheel gespecificeerd worden in termen van de geformaliseerde concepten en relaties. In deze interfaces vindt elke rol de voor die rol relevante gegevens en signalen terug. Zo kan een 'verwerkersinterface' worden gespecificeerd waarin verwerkers de gegevens kunnen ingeven, inzien, wijzigen en verwijderen die betrekking hebben op diens organisatie, de verwerkingen voor welke hij (mede)verantwoordelijk is, welke bewerkers namens hem verwerkingen mogen uitvoeren, enzovoorts. Ook kunnen in die interface signalen worden gespecificeerd, zoals verwerkingen die gebruikmaken van systemen van derden zonder dat die derde partij expliciet opdracht heeft de verwerking uit te voeren (artikel 12 Wbp) of zonder dat vaststaat dat de verwerkingsdoelen verenigbaar zijn met de doelen waarvoor de gegevens waren verkregen (artikel 9 Wbp). De laatste regel uit Figuur 3 laat zien hoe het signaal dat overtredingen artikel 7 Wbp signaleert, aan de rol van de verwerker wordt toegekend.

Als alle concepten, relaties en regels in ADL gespecificeerd zijn – zowel in relatie algebra als in natuurlijke taal –, en als de rollen en gebruikersinterfaces zijn gespecificeerd, dan is dit voldoende voor het genereren van een stuk prototypesoftware waarmee belanghebbenden in hun verschillende rollen, middels de voor hen beschikbare interfaces, gegevens kunnen invoeren en vervolgens alle (voor hen relevante) signalen gepresenteerd krijgen. Dit systeem wordt gebruikt om belanghebbenden aan den lijve te laten ondervinden welk effect de geformaliseerde regels hebben in verschillende usecases. Als deze effecten ongewenst zijn kan worden gediscussieerd over de juistheid van de regels waaruit deze effecten zijn ontstaan – deze zijn immers traceerbaar. Soms blijkt dat de geformaliseerde regels verbetering behoeven, maar het komt ook voor dat de belanghebbende de regel toch juist acht en bijgevolg de kennelijk onvoorziene maar wiskundig logische consequentie aanvaardt. Na een aantal verbeterslagen ontstaat een formalisatie waarvan de belanghebbenden zelf hebben vastgesteld dat deze in de praktijk de effecten heeft die zij ervan verwachten.

Als bij het formaliseren van de Wbp juristen (die deze wet goed kennen) als belanghebbenden optreden, dan wordt hiermee binnen de grenzen van het redelijke alle moeite gedaan om de Wbp goed te interpreteren en tot een goede formalisering ervan te komen. Van daaruit kunnen we een systeem genereren, dat we de 'privacyassistent' (PA) zullen noemen en dat van een gegevensver-

```
RULE "Integriteit van het verzamelen van persoonsgegevens" :
     I[Persoonsgegeven] |- verzamelDoel;verzamelDoel~
MEANING "Persoonsgegevens worden alleen verzameld ten behoeve van een (welbepaald,
uitdrukkelijk omschreven en gerechtvaardigd) doel (Artikel 7 Wbp)"
VIOLATION (TXT "Van persoonsgegeven '", SRC I, TXT "' is geen doel bekend waartoe het is
verzameld")
PURPOSE RULE "Integriteit van het verzamelen van persoonsgegevens" REF "Artikel 7 Wbp"
{+PERSOONSGEGEVENs worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde
doeleinden verzameld.-}
ROLE Verwerker MAINTAINS "Integriteit van het verzamelen van persoonsgegevens"
```

Figuur 3. Voorbeeld van de specificatie van een formele regel

zameling die een zekere verwerking betreft, elke inconsistentie en elke overtreding betreffende de geformaliseerde Wbp signaleert. Als de PA geen signalen (meer) afgeeft, kan op basis van het 'due diligence'-principe worden beargumenteerd dat de verwerking (op dat moment) aan de Wbp voldoet.

5 Een usecase

Om aan te tonen dat dit in principe mogelijk is, is door TNO een prototype gemaakt die deze eigenschappen demonstreert. Om het prototype te maken is eerst een (klein deel van) de Wbp geformaliseerd alsmede een aantal concepten en regels om IT-systemen mee te kunnen beschrijven. Daaruit is een prototype PA (PPA) gegenereerd die onvolledigheden of gebrek aan samenhang moet gaan signaleren. Om de werking hiervan na te gaan zijn eerst gegevens met betrekking tot een eerste verwerking ingevoerd en de signalen 'opgelost'. Daarna is een tweede verwerking gespecificeerd die voor een heel ander doel gebruikmaakt van delen van het eerste systeem ('function creep'). Er is gekeken welke signalen dit oplevert als we gegevens over deze uitbreiding aan het PPA aanbieden en of deze de verantwoordelijken en andere belanghebbenden ondersteunen bij het (weer) compliant worden aan de Wbp.

Als eerste verwerking postuleren we een (fictief) Deelnemers Localisatie Systeem (DLS), dat bestaat uit camera's en elektronische informatiezuilen in een (fictief) conferentieoord. Doel van het DLS is om op de informatiezuilen te tonen waar zich (ophopingen van) andere deelnemers bevinden op basis van een analyse van de camerabeelden.

Het DLS bestaat uit modules voor (1) het maken van (hoog resolute) camerabeelden door de camera's, (2) het opslaan van dit beeldmateriaal in een database, (3) het annoteren van de beelden, zoals het indiceren waar mensen op een beeld te zien zijn, (4) het converteren van hoog resoluut naar laag resoluut beeldmateriaal, (5) het anonimiseren van de annotaties en (6) het tonen van een kaart van (een deel van) het conferentieoord met daarop (geannoteerde) symbolen op de plaats waar zich deelnemers bevinden en de mogelijkheid tot het 'afspelen' van het laag-resolute beeldmateriaal. Doel van de verwerking is het informeren van deelnemers over waar zich activiteiten afspelen en hen in de gelegenheid stellen te zien wat daar gebeurd is.

Als tweede verwerking postuleren we een (fictief) Deelnemers Monitoring Systeem (DMS), dat is bedoeld om de bewaking te informeren zodra zich een incident voordoet, zoals iemand die flauwvalt of een persoon die zich niet als deelnemer heeft ingeschreven. Hierdoor kan het aantal veiligheidsmensen worden gereduceerd, terwijl de dienstverlening wordt verbeterd. Hiertoe worden modules (1), (2) en (4) van DLS hergebruikt en twee nieuwe modules geïntroduceerd: één voor het analyseren van het hoog resolute beeldmateriaal om voornoemde incidenten te detecteren en de tweede voor het afspelen van het hoog-resolute beeldmateriaal dat tot de incident-signalering heeft geleid. Het DMS maakt dus gebruik van modules van het DLS die daar oorspronkelijk niet voor waren bedoeld – een typisch geval van function creep.

Het invullen van de informatie over het DLS in de PPA levert niet alleen signalen op die betrekking hebben op het ontbreken van gegevens (zoals de verantwoordelijke, doelen, enzovoorts) maar maakt ook duidelijk hoe de verwerking in elkaar zit, welke modules met welke modules gegevens uitwisselen, wie de bewerkers (module verantwoordelijken) zijn enzovoorts. Omdat een deel van deze gegevens nodig is om een Wbp-melding te kunnen doen, ligt het voor de hand dat de PPA controleert of alle daartoe benodigde gegevens beschikbaar zijn en signaleert welke nog ontbreken.

Het invullen van de informatie over het DLS en DMS levert echter ook stof op voor discussies. Een daarvan betreft de grenzen van de verwerking. De module waar beeldmateriaal in wordt opgeslagen kan tot het DLS worden gerekend – die voorziet immers in het beeldmateriaal, maar ook tot zowel het DLS als DMS omdat beide dat beeldmateriaal gebruiken. Door beide keuzes in te vullen in de PPA merk je wat de gevolgen in termen van compliance zijn tussen deze keuzes. Zodoende draagt de PPA bij aan het duidelijk krijgen van alternatieven en het kiezen van de beste daaruit.

Een ander voorbeeld geldt doelbinding. Stel dat de video-opnamemodule als doel heeft 'hoog resoluut beeldmateriaal opnemen', de opslagmodule 'opslaan en ontsluiten van video's' en de andere modules soortgelijk hun doel is toegekend. De hiervoor al genoemde regel 'Elke module die een verwerking deels implementeert moet een doel nastreven dat een subdoel is van het doel van de verwerking' eist dan dat de doelen van de video-opnamemodule, de opslagmodule en de andere modules waaruit het DLS is opgebouwd, allemaal subdoelen moeten zijn van het DLS zelf: 'Het detecteren van de dichtheid van deelnemers op verschillende locaties en het publiceren ervan op bezoekerszuilen'. Dit kan niet automatisch worden vastgesteld, maar de verantwoordelijke kan dit wel. De PPA ondersteunt door te controleren of dit voor alle onderliggende modules het geval is.

Als we het DLS gaan uitbreiden met de DMS-modules wordt onmiddellijk duidelijk waar naar gekeken moet worden. Het doel 'detecteren van de dichtheid van deelnemers op verschillende locaties en het publiceren ervan op bezoekerszuilen' waartoe de videogegevens eerst zijn verzameld komt niet overeen met het doel van de DMS: 'het signaleren van incidenten ten behoeve van een optimale dienstverlening door de bewaking'. Doordat het PPA signaleert dat niet kan worden vastgesteld dat het doel waartoe de gegevens zijn verzameld overeenkomt met het doel waartoe ze worden verwerkt, wordt een concreet probleem van function creep zichtbaar. In onze case heeft dit ertoe geleid dat doelen veel preciezer werden geformuleerd en daarmee voor de betrokkenen veel duidelijker werd waartoe systemen bestaan.

Door het doel van module 2 te veranderen (in het specifiekere doel 'opslaan en ontsluiten van video's van hoge en lage resolutie') signaleert de PPA dat voor elke verwerking die de opslagmodule gebruikt weer moet

worden vastgesteld of deze nieuwe doelstelling een subdoel is van het verwerkingsdoel. Dit is een voorbeeld waar de PPA bijdraagt aan het herstellen van de consistentie van de informatie over het DLS (en DMS).

6 Mogelijkheden en beperkingen

Bij het invoeren van de informatie over specifieke DMS-modules, alsmede over die van het invoeren van het DMS zelf, zijn we aan alle kanten geholpen bij het inrichten van de verwerking zelf, de doelbindingen, enzovoorts. De informatie betreffende de verwerkingen is volledig en consistent zodra de PPA geen signalen meer geeft van het tegendeel. De signalerende functie is echter wel beperkt tot dat deel van de wet en dat deel van de IT dat is geformaliseerd. Deze beperking is echter geheel traceerbaar.

Een andere beperking is dat de PPA, net als de meeste andere geautomatiseerde tools, teksten niet inhoudelijk kan controleren. Of 'video opslaan en ontsluiten' wel een doel is, noch of dit als een geldig subdoel voor deze of gene verwerking kan worden aangemerkt, kan door de PPA worden gecontroleerd. Dat maakt de PPA alleen toepasbaar voor hen die de wet ook daadwerkelijk willen naleven. Eenieder die zich verlaat op informatie van de PPA die door een ander is ingevuld, dient zich derhalve te vergewissen van de betrouwbaarheid van die ander.

De PPA bevat alle gegevens voor een Wbp-melding. De verantwoordelijke zou pas een melding kunnen doen met die gegevens zodra de registratie zodanig is ingevuld dat er geen onvolledigheden of inconsistenties meer worden gesignaleerd. Dan immers is voldaan aan alle wettelijke regels die in de PPA zijn geformaliseerd.

Een interessante vraag is dan ook of een volledige PA wellicht onder de supervisie van (juristen van) het CBP ontwikkeld zou kunnen worden. Hun taak daarbij zou dan zijn om vast te stellen dat de PA niet alleen de juiste signalen geeft in de casuïstiek die zij in de praktijk tegenkomen, maar ook om – als de PA is 'goedgekeurd' – de bijbehorende documentatie te reviewen op juridische deugdelijkheid (binnen de grenzen van het redelijke). Dat dit kan heeft de praktijk reeds laten zien. Een dergelijke werkvorm is namelijk begin 2012 binnen de Raad voor de Rechtspraak toegepast voor het formaliseren van hun eigen werk [31]. Ook is op basis van de Wet justitiële en strafvorderlijke gegevens een prototype gemaakt voor ondersteuning van het proces voor het aanvragen van een Verklaring Omtrent het Gedrag (VOG), die bij JustID is gedemonstreerd [30].

Nadat voldoende is getest met de PA – door mensen in verschillende rollen – en de regels in dat proces zijn verbeterd, willen we graag van verwerkingen kunnen concluderen dat binnen de grenzen van het redelijke alle moeite is gedaan om zich ervan te vergewissen dat aan de wettelijke vereisten is voldaan. Dat de PA een (binnen de grenzen van het redelijke) getrouwe toets is van de wet die erin is geformaliseerd, blijkt dan enerzijds uit de testen die ermee zijn gedaan, maar anderzijds ook uit de documentatie die Ampersand hieruit kan genereren en is bedoeld om juristen ervan te overtuigen. Dat dit ook zo werkt is in het eerdergenoemde project bij de Raad voor de Rechtspraak in de praktijk gedemonstreerd [31].

Een andere interessante vraag is of de functionaliteit van een dergelijke PPA (bijvoorbeeld als een webservice) beschikbaar gesteld zou kunnen worden aan het mkb. Dit zou bijvoorbeeld huisartsen, onderwijsinstellingen, arbodienstverleners en dergelijke kunnen helpen om delen van de verwerkingen waarvoor zij verantwoordelijk zijn, te outsourcen binnen de grenzen van de privacywet- en regelgeving. Nog steeds komt het voor dat uit dit soort outsourcen privacyproblemen kunnen voortvloeien [4]. Door een dergelijke web-service te laten putten uit informatie die in het Wbp-meldingenregister aanwezig is, hoeven verantwoordelijken informatie over verwerkingen, die zij hergebruiken, niet (meer) in hun eigen administratie in te voeren: een simpele verwijzing ernaar volstaat, in de wetenschap dat als in die onderliggende informatie relevante delen worden gewijzigd, een signaal wordt afgegeven dat aangeeft wat nodig is om weer aan de wet te voldoen.

7 Conclusie

De Europese Commissie heeft voorstellen gedaan om de regelgeving rondom privacy flink aan te scherpen. Aantoonbaarheid van compliance hieraan en de in het vooruitzicht gestelde hoge boetes kunnen voor bedrijven die zwaar op IT leunen een serieus probleem worden. Deze problemen worden onder meer veroorzaakt door de toenemende complexiteit van wetten en systemen, 'function creep', de toenemende hoeveelheid 'open data' en het groeiende aantal individuen en mkb'ers die persoonsgegevens maken c.q. gebruiken. Door veranderingen in bijvoorbeeld wetgeving, systemen of gegevens(verwerkingen) kan een verwerking die vandaag compliant is, dat morgen niet meer zijn. Wij hebben een prototype privacyassistent gebouwd die, op basis van kennis over enerzijds de relevante privacywet- en regelgeving en anderzijds organisaties, hun processen en systemen, in staat is om informatie van concrete verwerkingen tot zich te nemen zoals die uit gangbare ontwerppraktijken voorhanden komt, en op basis daarvan te signaleren welke informatie over die verwerkingen nog ontbreekt of waar die inconsistent is. Deze signalen geven ofwel een overtreding van de wet aan, ofwel een ontbreken van informatie die nodig is voor aantoonbare compliance. Dit biedt ondersteuning voor partijen die aantoonbaar compliant willen worden en blijven. Dat geldt in het bijzonder ook wanneer gegevens over verwerkingen, doelen e.d. wijzigen, bijvoorbeeld door function creep. Dat hebben we laten zien door de PPA te gebruiken op een fictieve verwerking en daarop function creep toe te passen. Op basis van de opgedane ervaring lijkt het interessant te onderzoeken of het mogelijk is een 'privacyassistent' te bouwen die praktisch bruikbaar kan zijn, bijvoorbeeld als een webservice vanuit het CBP die mkb'ers helpt om met minimale inspanning aan de regelgeving te voldoen.

Referenties

1. Voorstel data protectie richtlijn', http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:NL:PDF, 2012.
2. Voorstel data protectie verordening', http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF, 2012.
3. Zembla: 'Privacy zieke werknemer niet gewaarborgd', http://zembla.vara.nl/Nieuws-detail.2624.0.html?&tx_ttnews[tt_news]=59700&tx_ttnews[backPid]=1974&cHash=454f7212e7d1101fcd5d7f802e66f294#, 2012.
4. Zembla: 'Honderdduizenden medische dossiers toegankelijk', http://zembla.vara.nl/Nieuws-detail.2624.0.html?&tx_ttnews[tt_news]=62103&tx_ttnews[backPid]=1974&cHash=ad611c3e125a72895e70e160eb5d35b9, 2012.
5. WebWereld: 'Lektober: maand van het privacylek', http://webwereld.nl/dossiers/8/lektober–maand-van-het-privacylek.html, 2011.
6. Security.nl: 'Populaire Android-apps stelen gevoelige gegevens', www.security.nl/artikel/43958/1/Populaire_Android-apps_stelen_gevoelige_gegevens.html, 2012.
7. CBP: 'Albert Heijn past privacybeleid "Mijn Bonus" aan na optreden CBP', www.cbpweb.nl/Pages/pb_20121112-ah-bonus-persoonsgegevens.aspx, 2012.
8. CBP: 'CBP vordert dwangsom NS in wegens bewaren reisgegevens studenten – NS heeft reisgegevens alsnog vernietigd en dwangsom betaald', www.cbpweb.nl/Pages/pb_20120613_cbp-dwangsom-ns-studenten-ov-chip.aspx, 2012.
9. Zenger: 'Wat niet weet, wat wél deert', https://www.bof.nl/2012/11/07/wat-niet-weet-wat-wel-deert/, 2012.
10. *Kamerstukken I* 2009/10, 30 312, N, Brief staatssecretaris betreffende de toekenning, het beheer en het gebruik van het Burgerservicenummer, https://zoek.officielebekendmakingen.nl/kst-30312-N.pdf, 2012.
11. S. Flight en P. v. E.: 'Hits en hints – De mogelijke meerwaarde van ANPR voor de opsporing', wodc.nl/images/volledige-tekst_tcm44-418513.pdf, 2011.
12. J.E.J. Prins, 'Function creep: over het wegen van risico's en kansen', in: M.P.C. Scheepmaker (red.), *Justitiële verkenningen*, p. 9-21, Wetenschappelijk Onderzoek- en Documentatiecentrum 2011.
13. N. Boot en E. W, 'Dutch Strategic Outsourcing Study: 2012', KPMG 2012.
14. NORA principe AP01: 'Diensten zijn herbruikbaar', www.noraonline.nl/wiki/Diensten_zijn_herbruikbaar, 2012.
15. S. Kulk en B. van L.: 'Brave New Open Data World?', *International Journal of Spatial Data Infrastructures Research* (7), 2012, p. 196-206.
16. T.D. Breaux e.a., 'Enforceability vs. accountability in electronic policies', aangeboden in juni 2006.
17. Travis D. Breaux en D.L. Baumer, 'Legally "reasonable" security requirements: A 10-year FTC retrospective', *Computers & Security* (30) 2011, p. 178-193.
18. R. Leenes e.a., *ENDORSE Deliverable D2.5 – Legal Requirements*, vsn 10.02, section 2.3, 2011.
19. H.L.A. Hart: *The Concept of Law*, Clarendon Press 1961.
20. G.A. Miller, 'The magical number seven, plus or minus two: some limits on our capacity for processing information', *Psychological review* (63) 1956, p. 81.
21. W. Teubert, *Meaning, Discourse and Society*, Cambridge University Press 2010.
22. Inspectie Veiligheid en Justitie, 'CIOT-bevragingen – Proces en rechtmatigheid', www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/11/24/ciot-bevragingen-proces-en-rechtmatigheid/lp-v-j-0000002077.pdf, 2012.
23. H. Blokpoel, 'Compleet veranderen in ontspannen tempo', *Ordina Annual Magazine* 2008, p. 16-19.
24. Algemene Rekenkamer, 'Immigratie- en Naturalisatiedienst', www.rekenkamer.nl/dsresource?objectid=67140&type=org, 2005.
25. S. Dobbelaar, 'De IND neemt de regels in eigen handen!', www.lac2010.nl/Uploads/Files/Plenair_20II_20-_20Dobbelaar_2c_20S.pdf, 2010.
26. NAF-architectuurprijs 2009: de IND', www.naf.nl/nl/naf-prijzen/2009_paul_teeuwen_en_de_ind.html, 2009.
27. Kamerbrief derde voortgangsrapportage INDiGO', www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/10/04/kamerbrief-derde-voortgangsrapportage-indigo/kamerbrief-derde-voortgangsrapportage-indigo.pdf, 2012.
28. *Audit INDiGO 'Willen, kunnen en doen*, KPMG Advisory 2011.
29. S. Joosten, L. Wedemeijer en G. Michels, *Rule Based Design*, Open University of the Netherlands 2010.
30. R Joosten en S.J.: *VOG demo voor JustID*, 2012.
31. *Project Koppelvlak: Eén wet, één waarheid: Een semantisch model voor de Rechtspraak*, Raad voor de Rechtspraak 2012.