Meer dan compliance en informatiebeveiliging

Privacy

3 mei 2017

De Nederlandse privacywetgeving volgens de Europese Richtlijn 95/46/EG en de daarop gebaseerde Wet bescherming persoonsgegevens (Wbp) zijn bijna net zo oud als de jubilerende NOREA. De IT-auditor die privacyvraagstukken beoordeelt ontleent zijn normatieve raamwerk grotendeels aan deze wet- en regelgeving, en in het verlengde daarvan aan het domein van informatiebeveiliging. Nu, na twintig jaar ervaring met de richtlijn, hebben we te maken met een nieuwe Europese verordening die als doel heeft een betere privacybescherming te leveren. Kunnen IT-auditors hier de komende jaren mee uit de voeten, of is er misschien nog meer nodig (en wat dan)?

In dit artikel betogen we dat het voor een zorgvuldige belangen- en risicoafweging in privacyvraagstukken belangrijk is dat de IT-auditor ook de fundamentele principes en andere invalshoeken van privacy in zijn beschouwingen betrekt.

Privacy wat de klok slaat

Privacy staat in de schijnwerpers. Er gaat geen dag voorbij zonder nieuws op het gebied van de bescherming van onze persoonsgegevens. In 2016 was er in Nederland buitengewoon veel aandacht voor dit thema. Zie hiervoor het tekstkader 'Privacy in Nederland, 2016: enkele voorbeelden'.

Kader 1: Privacy in Nederland, 2016: enkele voorbeelden

- Op 1 januari wordt de Wet Meldplicht Datalekken van kracht, die organisaties in de publieke en private sector verplicht om in bepaalde gevallen lekken van persoonsgegevens te melden aan de Autoriteit Persoonsgegevens en (soms ook) aan de betrokken personen.
- In april is er veel discussie over de kabinetsplannen voor wetswijzigingen die diensten als MIVD, AIVD, maar ook opsporingsdiensten ruimere bevoegdheden moeten geven of informatie 'te tappen', en providers moeten verplichten metadata preventief vast te leggen.
- In mei wordt EU-breed de nieuwe Algemene Verordening Gegevensbescherming (ofwel General Data Protection Regulation – GDPR) van kracht, die vanaf mei 2018 van toepassing zal zijn en de Europese Dataprotectie Richtlijn (en daarmee de Wet Bescherming Persoonsgegevens) zal vervangen.
- In september stemt de Tweede Kamer in met een wetsvoorstel van minister Schippers om zorgverzekeraars onder bepaalde omstandigheden toegang te geven tot medische dossiers met het oog op het terugdringen van fraude bij ziektekostendeclaraties. Dit leidt tot veel ophef omdat volgens tegenstanders van de wet hiermee de vertrouwelijkheid van medische persoonsgegevens wordt geschonden.
- Eveneens in september pleit AIVD-voorman Bertholee in de Volkskrant voor een inperking van encryptie van communicatie met toepassingen als Whatsapp, omdat versleuteling van communicatie op gespannen voet zou staan met het beschermen van de rechtsorde. Dit leidt tot een (hernieuwde) discussie over de balans tussen privacy en veiligheid.
- In oktober besteedt televisiezender NPO 3 twee weken lang uitgebreid aandacht aan privacy onder de noemer 'Privacyweken'.

Het is buiten de context van dit artikel om diep in te gaan op de oorzaken van deze grote belangstelling, maar de volgende aspecten spelen daarin zeker een rol:

- Technologische ontwikkelingen maken het op grote schaal aanleggen van gegevensverzamelingen over individuen steeds gemakkelijker en goedkoper.
- Het is (daarmee) steeds eenvoudiger om individuen te profileren en op basis daarvan analyses en voorspellingen te doen, bijvoorbeeld over kredietwaardigheid, gezondheid, et cetera.
- Bedrijven en overheden spannen zich om verschillende redenen, zoals een beoogde verbetering van hun dienstverlening, meer en meer in om de beschikking te krijgen over gegevens van individuen.
- Er is een toename van (publiciteit over) incidenten waarbij sprake is van misbruik van persoonsgegevens; denk aan identiteitsfraude.
- Surveillance en data-analyse spelen een belangrijke rol in de actuele (maatschappelijke) veiligheidsdreiging en de adequate bestrijding van crimineel gedrag en terrorisme.
- Burgers zijn zich, door bovengenoemde factoren en door de activiteiten van privacywaakhonden en actiegroepen, in toenemende mate bewust van het belang van een ongeschonden persoonlijke levenssfeer en de waarde van hun persoonsgegevens.

Privacy en de IT-auditor

Het opstomende privacyschip neemt in zijn kielzog twee andere kennisgebieden mee. Op de eerste plaats is dat informatiebeveiliging. Immers, het waarborgen van privacy vereist de bescherming van gegevens, en die deskundigheid ligt van oudsher bij professionals op het gebied van informatiebeveiliging. Ten tweede is er het juridische domein. Zeker in Europese Unie is de wetgeving een uiterst belangrijk aanknopingspunt voor organisaties die met persoonsgegevens omgaan, voor de betrokkenen zelf, en voor toezichthouders. Dat die wetgeving bovendien aan verandering onderhevig is versterkt de aandacht voor privacy alleen maar.

De IT-auditor heeft bij het uitvoeren van zijn assurance- en adviesdiensten met privacyvraagstukken te maken en bovenstaande twee aspecten – informatiebeveiliging en compliance – liggen op een voor hem bekend terrein. Een IT-auditor is thuis in kwesties die met de beveiliging van gegevens te maken hebben, zeker in een geautomatiseerde omgeving. Waar het gaat om compliance zal de IT-auditor zich verdiepen in de (veranderende) wet- en regelgeving en die een plaats geven in zijn normatieve raamwerk.

In essentie gaat het bij privacybeslissingen om een zorgvuldige afweging van (vaak tegengestelde) belangen en risico's, en de verhoogde maatschappelijke aandacht voor privacy onderstreept het belang hiervan. Voor de IT-auditor is het een uitdaging en biedt het kansen. Om die optimaal te kunnen benutten moeten IT-auditors bij het geven van assurance of advies over privacyvraagstukken echter niet volstaan met aandacht voor informatiebeveiliging en compliance met wetgeving. Privacy is een complex begrip dat meer is dan de optelsom van een juridisch kader en de beveiligingsmaatregelen om dat kader te implementeren. Als de IT-auditor een stapje verder en een laagje dieper gaat en zich rekenschap geeft van dit fundamentelere privacybegrip en van de maatschappelijke waarden waar het uit voortkomt zal hij in privacykwesties nog meer waarde kunnen toevoegen, door ook vragen te beantwoorden als: zijn bij een bepaalde verwerking van persoonsgegevens de relevante dilemma's voldoende onderkend vanuit verschillende gezichtspunten, en zijn de belangen die daarbij spelen voldoende afgewogen? Is de verwerking van persoonsgegevens in overeenstemming met de geest van de privacybeginselen, en niet alleen met de letter van de wet? Met andere woorden, de IT-auditor kan dan niet alleen antwoord geven op de vraag 'mag het?' maar ook op 'moet je dit willen?'

> *"Niet alleen antwoord geven op de vraag 'mag het?' maar ook op 'moet je dit willen?'"*

We bespreken in dit artikel een aantal facetten van privacy die niet onderbelicht mogen blijven gegeven de actuele aandacht voor de wetgeving en de veranderingen daarin: respectievelijk WBP en AVG. We zullen achtereenvolgens ingaan op:

- privacy en privacyprincipes;
- privacy en security;
- privacy als economisch vraagstuk;
- de effectiviteit van privacywetgeving.

Deze facetten kunnen worden gezien als metaforische 'lenzen', waardoor een privacyvraagstuk vanuit verschillende perspectieven kan worden bekeken. Dit kan de analyse en de kwaliteit van de oplossing verrijken. De lenzen die we in dit artikel ten tonele voeren zijn geenszins limitatief; het is denkbaar dat bij bepaalde privacyvraagstukken aanvullende afwegingen worden gemaakt, bijvoorbeeld op basis van een ethische lens of een 'nationale veiligheidslens'. Waar het ons om gaat is dat een IT-auditor, ongeacht zijn specifieke opdracht of opdrachtgever, zich bewust is van de wenselijkheid om privacyvraagstukken vanuit meerdere invalshoeken te benaderen om te komen tot een zorgvuldige(r) afweging van (vaak tegengestelde) belangen en risico's.

Weinig tijd? **Klik op deze link door naar de adviezen en take-aways**. De onderbouwing volgt hieronder.

Privacy en privacyprincipes

Privacy is een breed begrip dat verschillende dimensies kent. Zo spreekt men van lichamelijke privacy (zelfbeschikking over het eigen lichaam), territoriale privacy (beperkingen op de inbreuk op iemands fysieke omgeving, zoals huis of werkplek), communicatieprivacy (denk aan het briefgeheim) en informationele privacy (het verzamelen en verwerken van persoonsgegevens). [SWIR12] Bij het schrijven van dit artikel hadden we deze laatste dimensie van privacy in gedachten, wat overigens niet betekent dat onze argumenten voor andere vormen van privacy niet zouden gelden.

In 1890 definieerden de Amerikaanse juristen Warren en Brandeis in een beroemd geworden artikel privacy als 'het recht om met rust gelaten te worden'. [WARR90] In de loop van de tijd zijn er nog talloze definities van privacy gepubliceerd. Zo definieert de Verenigde Naties in een verklaring over massamedia en de rechten van de mens privacy als: 'het recht zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf'. In dit artikel hanteren we de volgende definitie voor privacy, omdat die sterk de nadruk legt op het zelfbeschikkingsrecht van een individu waar het gaat om zijn persoonsgegevens:

'Een individu moet zelf moeten kunnen bepalen én invloed kunnen uitoefenen op het soort en de hoeveelheid informatie die over hen bekend is bij, en gebruikt wordt door anderen.' [NASA01]

In Europa is privacy als recht verankerd in het Europees Verdrag voor de Rechten van de Mens (EVRM). Artikel 8 van dit verdrag stelt: 'Een ieder heeft recht op respect voor zijn

privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie'. Het EVRM, en in het bijzonder dit artikel staan aan de wieg van veel privacywetgeving binnen de Europese Unie. Een daarvan is de Europese richtlijn 95/46/EG van het Europees Parlement en de Europese Raad, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Deze richtlijn trad in december 1995 formeel in werking en heeft een tweeledig doel. Enerzijds beoogt de richtlijn de privacy van individuen te beschermen in een samenleving waarin steeds meer gegevens op een geautomatiseerde manier worden verwerkt (hieronder valt ook het verspreiden van persoonsgegevens). Kortom, het beschermen van privacy als fundamenteel mensenrecht in het verlengde van de EVRM. Anderzijds is het een doel om consistentie te creëren in de privacywetgeving van de EU-landen met het oog op het optimaal functioneren van de interne markt. [EURL00]
Aangezien de richtlijn geen directe werking had maar geïmplementeerd moest worden in nationaal recht (in Nederland de Wbp), heeft ook 95/46/EG verschillende interpretaties en implementaties van wetgeving in de lidstaten niet kunnen voorkomen. [USTA12] Dit is een van de redenen waarom de Europese Unie in mei 2016 met een nieuwe wet is gekomen: de Algemene Verordening Gegevensbescherming (AVG), die de volgende stap is in de harmonisatie van privacyregelgeving, de bescherming van persoonsgegevens en bevordering van vrij verkeer van gegevens binnen de Unie. [OVER16] De verordening is nu al van kracht maar organisaties hebben tot mei 2018 de tijd om aan de nieuwe richtlijnen te voldoen. Het karakter van een verordening brengt met zich mee dat een groot deel van de bepalingen rechtstreekse werking heeft en geen omzetting in nationaal recht behoeft. Dit zal naar verwachting de verschillen in interpretaties van de wet reduceren en bijdragen aan de kwaliteit van de bescherming én het vrije verkeer van persoonsgegevens binnen de Europese Economische Ruimte. De Autoriteit Persoonsgegevens beschrijft op haar website de grootste veranderingen die de AVG teweeg zal brengen: versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties en stevige bevoegdheden voor alle Europese privacytoezichthouders. [AUTO16a]
De EU-richtlijn én de AVG zijn beide gebaseerd op (en te herleiden naar) een aantal basisprincipes. De Organisation for Economic Co-operation and Development (OECD) publiceerde deze basisprincipes in 1980 en ze hebben wereldwijd navolging gevonden als uitgangspunt voor privacyraamwerken. Hieronder zullen deze principes kort de revue passeren.

- Dataminimalisatie. Persoonsgegevens moet worden verzameld binnen de wettelijke grenzen en waar mogelijk met toestemming van de betrokkenen. Daarnaast geldt dat men zoveel persoonsgegevens moet verzamelen als nodig is voor een goede bedrijfsvoering maar zo weinig als mogelijk ter bescherming van de privacy van betrokkenen.
- Datakwaliteit. Persoonsgegevens die verwerkt worden moeten relevant zijn voor het doel waarvoor ze zijn verkregen, compleet en nauwkeurig zijn en up to date gehouden worden waar mogelijk.
- Doelbinding. Ten tijde van het verzamelen van de persoonsgegevens moet het doel van de verwerking gespecificeerd worden. Verder gebruik, voor zover niet met het doel verenigbaar, is niet toegestaan.

- Gebruiksminimalisatie.Persoonsgegevens mogen niet openbaar gemaakt worden, ter beschikking gesteld worden of gebruikt worden voor andere doeleinden (zie principe van doelbinding) dan waarvoor de data initieel is verzameld.
- Beveiliging. Persoonsgegevens moeten een redelijke bescherming genieten tegen onder meer verlies, diefstal, vernietiging, toegang, wijziging en ondeugdelijk gebruik.
- Transparantie. Er moet een beleid van openheid zijn over ontwikkelingen, uitvoering en beleid voor persoonsgegevens. Daarnaast moet transparant gecommuniceerd worden over het verwerken van persoonsgegevens, de doelen van het gebruik en het soort persoonsgegevens dat wordt verwerkt. Tot slot moet de identiteit en verblijfplaats van de verwerker van persoonsgegevens bekend zijn.
- Rechten van betrokkenen. Betrokkenen moeten het recht hebben om informatie te krijgen of er al dan niet persoonsgegevens van hen worden verwerkt en, indien terecht, deze te corrigeren, wissen of aan te vullen.
- Verantwoordelijkheid. Verwerkers van data hebben de verantwoordelijkheid om bovenstaande principes na te komen door maatregelen hiervoor te nemen.

Hoewel elk principe van fundamenteel belang is voor een goed privacyraamwerk, is er een aantal dat de IT-auditor met name zal aanspreken, zoals de beveiliging en datakwaliteit van persoonsgegevens. Die aspecten bieden immers een voor hem vertrouwd perspectief. De IT-auditor doet er echter verstandig aan zich niet tot deze principes te beperken. Wij denken dat hij meer toegevoegde waarde kan leveren door bij zijn activiteiten juist ook aan de andere principes nadrukkelijk aandacht te besteden. De IT-auditor moet dan vaststellen dat:

- er niet méér gegevens worden verwerkt dan strikt noodzakelijk voor het doel (dataminimalisatie);
- de organisatie technisch in staat is om aan een informatieverzoek van een betrokkene te voldoen (rechten van betrokkenen);
- toegang tot persoonsgegevens alleen op basis van het ‘need to know’ principe wordt verleend, zodat de persoonsgegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn verzameld (gebruiksminimalisatie en doelbinding).

Ook de beginselen van proportionaliteit en subsidiariteit kunnen onderwerp van toetsing zijn. Hierbij worden vragen gesteld als: is het middel waarvoor wordt gekozen evenredig aan het doel dat men wil bereiken (proportionaliteit)? En zijn er minder ingrijpende manieren mogelijk om hetzelfde doel te bereiken (subsidiariteit)? De antwoorden op deze vragen leveren in samenhang met de toetsing van de beveiliging en kwaliteit van de data, een vollediger beeld op van de overwegingen die bij een privacybeslissing een rol spelen, doen recht aan de onderliggende principes van de privacywetgeving, en zijn een belangrijke stap om niet alleen compliant met de wet te zijn, maar vooral een goed huisvaderschap over persoonsgegevens te kunnen voeren.

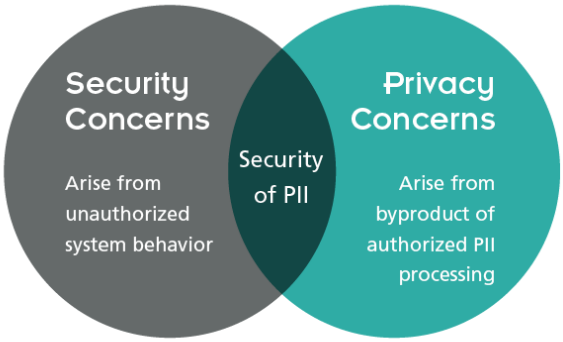
Privacy en security

Zoals eerder in dit artikel is opgemerkt, speelt informatiebeveiliging ('security') in privacyvraagstukken een centrale rol. Het is geen toeval dat datakwaliteit en beveiliging tot de privacyprincipes van de OECD behoren.[1] In de titel van de wet die ons allemaal bezighoudt – de AVG – komt de term 'privacy' niet voor, maar wordt gesproken van 'gegevensbescherming/data protection'. Dat riekt meer naar een beveiligingsdoelstelling dan naar een mensenrecht. Privacy en informatiebeveiliging zijn sterk verwant, maar niet aan elkaar gelijk. Het is verstandig bij de overeenkomsten en verschillen tussen de twee begrippen stil te staan.

Bambauer pleit ervoor deze concepten duidelijk uit elkaar te houden. [BAMB10] In zijn visie is privacy een vraagstuk waarbij een maatschappij fundamentele, waardengestuurde en normatieve keuzes maakt over wie toegang tot bepaalde (persoons)gegevens moet hebben. Privacy gaat, met andere woorden, om de verdeling van macht ('power') over informatie. Security daarentegen is de implementatie van die macht, met maatregelen die genomen worden om ervoor te zorgen dat daadwerkelijke toegang tot informatie in overeenstemming is met de privacykeuzes die de maatschappij heeft gemaakt. Een datalek is in deze redenering geen privacyvraagstuk, maar een beveiligingsissue met consequenties voor de privacy van betrokkenen. De fundamentele keuzes over wat tegen wie moet worden beschermd, worden immers door dat lek niet aangetast; het is de implementatie van de keuzes die tekortschiet. Bambauer noemt privacy-issues een zero-sum game, waarbij het gaat om keuzes over machtsverdeling tussen maatschappelijke actoren en waarbij het voordeel voor de één altijd gelijk is aan het nadeel voor de ander. Problemen met de beveiliging van persoonsgegevens schaden daarentegen zowel de betrokkene (het individu) als de houder van die gegevens. De eerste, omdat zijn gegevens in verkeerde handen vallen, de tweede omdat hij reputatieschade, boetes, en omzetverlies riskeert.

Koops bespreekt 'privacy' en 'informatieveiligheid' als twee zijden van dezelfde munt. [KOOP14a] Ze dienen vergelijkbare doelen en vragen om een vergelijkbare aanpak. Niettemin signaleert hij enkele wezenlijke verschillen tussen de twee begrippen. Zo is privacy in Koops' zienswijze in de benadering van het object meer zwart-wit: na de vaststelling dat een bepaald informatie-item een persoonsgegeven is, is de behandeling daarvan in principe gelijk, terwijl informatieveiligheid meer – op risico's gebaseerde – granulariteit in de beveiliging van informatie-items voorstaat. Daarnaast zijn er verschillen in de omvang van de beschermende maatregelen, en in de manier waarop tegen het delen van informatie wordt aangekeken. Koops pleit voor een aanpak waarin het gemeenschappelijke doel van een 'propere informatiehuishouding' wordt nagestreefd en zowel privacy als informatieveiligheid een prominente plaats op de beleidsagenda's van organisaties krijgen.

In de Verenigde Staten heeft het National Insitute of Standards and Technology (NIST) recent een rapport gepubliceerd dat de relatie tussen informatiebeveiliging en privacy expliciet probeert te maken. [NIST17] In het rapport wordt onderkend dat beveiligingsissues en privacy-issues elkaar weliswaar kunnen overlappen, maar dat veel privacy-issues een nevenproduct kunnen zijn van specifiek geautoriseerde verwerking van persoonsgegevens. Dit is zichtbaar gemaakt in het venndiagram in figuur 1. Hierbij staat 'PII' voor 'Personally Identifiable Information': persoonsgegevens.

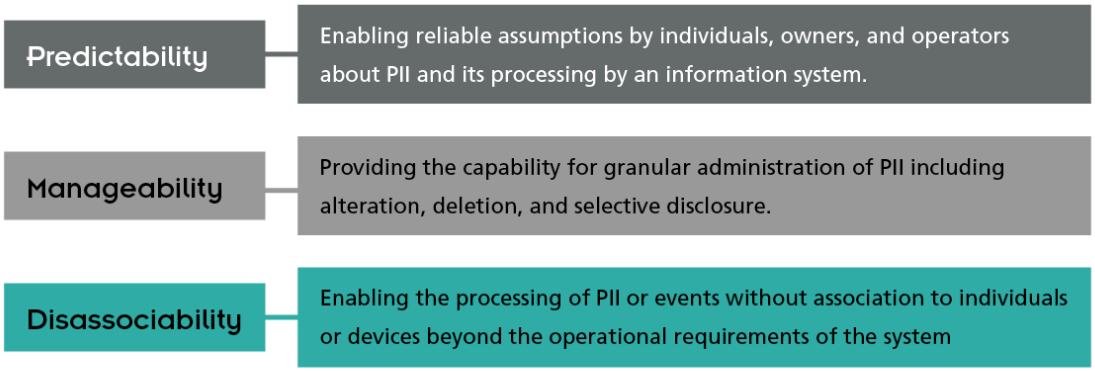


FIGUUR 1. RELATIE TUSSEN INFORMATIEBEVEILIGING EN PRIVACY (BRON: [NIST17])

Voor ons betoog is met name het grote segment van de rechtercirkel relevant. Hier is sprake van privacyrisico's die zich voordoen zelfs als de verwerking van de betreffende persoonsgegevens geautoriseerd is. Met andere woorden: ook in een situatie van compliance met wet- en regelgeving bestaan er resterende privacyrisico's die aandacht verdienen en die bij een benadering die zich met name richt op informatiebeveiliging niet vanzelfsprekend worden geadresseerd. Die risico's liggen op gebieden als:

- verlies van vertrouwen van individuen in de organisatie die persoonsgegevens verwerkt;
- discriminatie, stigmatisatie, machtsongelijkheid;
- verlies van zelfbeschikking en vrijheid;
- economische schade.

Vervolgens stellen de auteurs voor om privacy te incorporeren als een attribuut van betrouwbare systemen (*'trustworthy systems'*), en formuleert het rapport een aantal doelstellingen voor privacy engineering naar analogie van de drievoudigheid van *confidentiality-integrity-availability* (CIA) bij reguliere informatiebeveiligingsvraagst ukken. Die doelstellingen luiden *predictability-manageability-disassociability*, ofwel: voorspelbaarheid-beheersbaarheid-dissocieerbaarheid (zie figuur 2).



FIGUUR 2. DOELSTELLINGEN VAN PRIVACY ENGINEERING (BRON: NIST)

Voor een uitgebreide beschrijving van deze doelstellingen verwijzen we kortheidshalve naar het rapport. NIST merkt op dat de doelstellingen gebruikt kunnen worden om de kloof te dichten tussen high-level privacyprincipes en de implementatie van die principes in systemen. Dit raakt natuurlijk ook aan *privacy by design* and by *default*, zoals de AVG vereist.
Het onderscheid tussen privacy en informatiebeveiliging, zoals hierboven vanuit verschillende invalshoeken beschreven, heeft voor de IT-auditor praktisch nut. Beveiligingsvraagstukken liggen voor de IT-auditor op bekend terrein en zijn om die reden

met zijn standaardinstrumentarium beet te pakken. Privacy-issues overlappen slechts ten dele met security-issues. Ze hebben een eigen risicoprofiel, zijn vaak normatiever van karakter, moeilijker in een goed/fout-context te plaatsen en vereisen soms lastige keuzes met potentieel grote impact. In 2014 ontstond ophef toen ING een proef wilde starten waarbij klanten aanbiedingen van derde partijen zouden ontvangen op basis van betaalgedragprofielen. Hier was niet zozeer sprake van een security-issue als wel van een specifiek privacyvraagstuk. Plotseling ontstond de indruk dat retailers de beschikking zouden krijgen over klantgegevens en dat de bank daaraan zou verdienen. Dat bracht flinke maatschappelijke reuring met zich mee, terwijl er geen sprake was van non-compliance met de wet noch van een beveiligingsincident. ING gaf toe dit niet te hebben voorzien. Had de bank zich bedacht als er een IT-auditor bij deze beslissing betrokken was geweest? Wellicht, maar dan had die IT-auditor het vraagstuk in elk geval vanuit een andere invalshoek moeten benaderen dan alleen op basis van informatiebeveiliging of compliance. Privacykeuzes vereisen fundamentele vragen vanuit verschillende perspectieven en de IT-auditor zou die vragen moeten stellen.

Privacy als economisch vraagstuk

In het voorwoord bij haar jaarverslag over 2016 spreekt de Autoriteit Persoonsgegevens expliciet over 'de vermarkting' van persoonsgegevens en de toenemende rol van persoonsgegevens als betaalmiddel. [AUTO15b] De toezichthouder plaatst persoonsgegevens hiermee duidelijk in een transactionele sfeer en in een economische context. Het is interessant hier wat uitgebreider bij stil te staan.

Al jarenlang bestudeert de wetenschap privacy ook vanuit een economische invalshoek. Persoonsgegevens worden daarbij gezien als een schaars goed op een markt van aanbieders en vragers (zoals individuen respectievelijk bedrijven). Die worden geconfronteerd met alternatieven en moeten keuzes maken over privacy om hun behoeften zo goed mogelijk te bevredigen. Persoonsgegevens hebben een prijs, en een bepaalde *trade off* tussen geheimhouding en openbaarheid van persoonsgegevens brengt voor beide partijen zowel opbrengsten als kosten met zich mee. Is in zo'n situatie een evenwicht denkbaar en hoe ziet dat eruit? Dat is de vraag waarmee privacy-economen zich bezighouden.

Vooral in de sterk ex-ante gereguleerde Europese situatie is bescherming van persoonsgegevens bijna een doel op zichzelf geworden: hoe strakker de beveiliging van persoonsgegevens, des te beter, zo lijkt het uitgangspunt. Kenmerkend voor de economische benadering is dat die zo'n veronderstelling loslaat en uitgaat van rationeel handelende actoren op zoek naar een economisch optimum. Met andere woorden: we schuiven het stereotiepe beeld van de kwetsbare burger, die tegen de machtige Googles, Facebooks en kwaadwillende overheden beschermd moet worden terzijde en zien die partijen als gelijkwaardige participanten op een markt, in staat om hun eigen afwegingen te maken en privacybeslissingen te nemen zonder grote bemoeienis van wetgevers of marktregulerende instanties. Een dergelijke economische benadering van privacyvraagstukken is niet de meest voor de hand liggende modus operandi voor IT-auditors, maar ook hier geldt dat ze wel degelijk kan bijdragen aan het inzicht dat die kan verschaffen en daarmee aan de kwaliteit van privacybeslissingen waarbij de IT-auditor is betrokken.

Niet dat de privacy-economen het altijd met elkaar eens zijn overigens. Zeker in de begindagen van discussie was, onder invloed van de neoklassieke *Chicago School*-economen, de mening nogal prominent dat elke beperking van de toegang tot persoonsgegevens het bereiken van een optimale marktsituatie in de weg zou staan. Zowel de aanbieder (het individu) als de vrager naar persoonsgegevens (een bedrijf of andere organisatie) zou het beste af zijn met volledige transparantie en openheid. Daar wordt inmiddels veel genuanceerder over gedacht. In een economische context zal een individu de waarde van zijn persoonsgegevens moeten bepalen om rationele beslissingen te kunnen nemen over het wel of niet openbaar maken van die gegevens. Acquisti [ACQI10] geeft drie factoren die deze rationaliteit in de weg staan:

Onvolledige informatie. Zo weet een consument in veel gevallen niet wat er met zijn persoonsgegevens (verder) gebeurt nadat hij deze aan een andere partij heeft geopenbaard.

Beperkte cognitieve vermogens om beschikbare informatie adequaat te verwerken. Denk hierbij bijvoorbeeld aan uitgebreide en ingewikkelde privacyvoorwaarden en -statements van bedrijven.

Systematische afwijkingen van rationele besluitvorming. Denk hierbij aan het klakkeloos accepteren van (privacy)voorwaarden bij een impulsieve of haastige internettransactie.

Kort gezegd: de veronderstelling van rationeel gedrag die de Chicago School veronderstelde kent belangrijke beperkingen. Niettemin blijft de economische benadering van privacy zoeken naar een optimale balans met in het achterhoofd: *having too much privacy can be as bad as having too little.* [STRA13]

Geformuleerd in economische terminologie zijn wij er in de Europese context aan gewend om over privacy voornamelijk te spreken als (a) de kosten en negatieve effecten die een individu ondervindt van het verstrekken (openbaar maken) van persoonsgegevens, versus (b) de opbrengsten en voordelen die bedrijven ondervinden met de aan hen toevertrouwde persoonsgegevens. Voor IT-auditors die een bijdrage moeten leveren aan privacyvraagstukken is de economische benadering, alhoewel op zichzelf onvoldoende voor een gebalanceerde belangenafweging, heel interessant. Zij vult het plaatje aan en geeft daarmee een vollediger beeld van privacy-afwegingen die gemaakt kunnen en moeten worden. Ze onderkent bijvoorbeeld dat een individu ook substantiële voordelen heeft bij het delen van persoonsgegevens, en dat bedrijven anderzijds kosten en nadelen ondervinden als zij de beschikking krijgen over die gegevens. Acquisti werkt dit gedetailleerder uit. [ACQI10] Op basis daarvan hebben we in onderstaande tabel, indicatief en niet uitputtend, een aantal voorbeelden uit zijn artikel bewerkt, aangevuld en verwerkt.

Ter toelichting, er zijn twee actoren: degene op wie de persoonsgegevens betrekking hebben *('data subject'*) en degene die daar belangstelling voor heeft (*'data holder',* in het Nederlands aangeduid als 'verwerkingsverantwoordelijke'). De persoonsgegevens kennen twee statussen: door het data subject verstrekt aan de data holder (*'disclosed'*) en niet verstrekt (*'undisclosed'*).

	Data subject		Data holder	
	Kosten/nadeel	Opbrengst/voordeel	Kosten/nadeel	Opbrengst/voordeel
Disclosed data	• Onzekerheid over toekomstige impact van disclosure ('blanco cheque') • Risico van identiteitsfraude en ander misbruik • Negatieve prijsdiscriminatie • Uitsluiting • Opportunity costs bij doorverkoop door holder • Gevoel van kwetsbaarheid, onveiligheid, onrust	• Kortingen • Gepersonaliseerde aanbiedingen • Cross-platform services • Positieve prijsdiscriminatie • Verhoogd gebruiksgemak • Eenvoudiger toegang tot faciliteiten (financiering, verzekering) • Macro-economische effecten: veiligheid, gezondheid	• Kosten van gegevensverzameling en beheer • Sancties en verlies van klanten bij non-compliance of datalekken • Opportunity costs ex-ante verlies van klanten • Investeringen in beveiligingsinfra	• Marketingvoordelen • Extra opbrengsten door gerichte aanbiedingen • Indirecte opbrengsten door wederverkoop persoonsgegevens • Betere taakuitvoering (denk aan opsporing, criminaliteit- en fraudebestrijding)
Undisclosed data	• Kosten van toepassing maatregelen die privacy waarborgen • Opportunity costs van voordelen bij disclosure persoonsgegevens	• Ongevoelig voor misbruik persoonsgegevens	• Toetredingsbarrière tot markt • Minder innovatiemogelijkheden	• Niet kwetsbaar voor datalekken en gevolgen daarvan • Positief privacy-imago

TABEL 1. KOSTEN EN OPBRENGSTEN VAN HET (NIET) DELEN VAN PERSOONSGEGEVENS (LOSJES GEBASEERD OP [ACQI10])

Actuele discussies over het delen van persoonsgegevens spelen zich sterk af in de groen gearceerde gebieden. Een bepaalde privacy-afweging zou aan kracht winnen als beslissers (én de IT-auditor) ook expliciet aandacht besteden aan de inhoud, en waar mogelijk kwantificering, van de andere cellen.

Effectiviteit van wetgeving

Ons betoog is erop gericht IT-auditors te stimuleren bij privacyvraagstukken verder te kijken dan alleen naar compliance- en informatiebeveiliging, omdat er andere invalshoeken zijn die samen met compliance en informatiebeveiliging een completer beeld geven op privacybeslissingen. Een argument om dat te doen kan ook worden gevonden in de effectiviteit van de wetgeving op het gebied van de bescherming van persoonsgegevens.
De Europese privacywetgevingssituatie is *comprehensive.* Zowel de Richtlijn 95/46/EG als de AVG gaan uit van een juridische *one size fits all*-benadering die een optimale bescherming van persoonsgegevens in de lidstaten moet garanderen, terwijl gelijktijdig het functioneren van de interne markt moet worden gestimuleerd. Er kunnen belangrijke vraagtekens worden gezet bij de effectiviteit van een benadering waarin de wet zo'n prominente en centrale rol heeft. Als die vraagtekens terecht zijn en de wetgeving als belangrijk middel voor het halen van maatschappelijke privacydoelen tekortschiet, dan zal een focus op compliance met die wet onvoldoende zijn om betere privacy voor burgers te bewerkstelligen.
Koops stelt dat *'the direction of the data protection reform* (lees: de AVG) *is fundamentally flawed'*. [KOOPS14b] Hij noemt drie belangrijke tekortkomingen die het behalen van de doelstellingen van de AVG in de weg zullen staan:

- De misconceptie dat gegevensbeschermingswetten kunnen bijdragen aan informationele zelfbeschikking van individuen.
- (Aanvullende) wetten maken taken (met name van data holders) niet eenvoudiger, maar juist complexer.
- Eén alomvattende wet rekt gegevensbescherming uit tot het breekpunt en maakt haar betekenisloos.

Ter onderbouwing hiervan stelt Koops onder andere, dat controllers (data holders) geen intentie hebben om het verzamelen van persoonsgegevens te limiteren tot een noodzakelijk minimum, en waarschuwt hij voor een situatie waarin voorgeschreven maatregelen zoals een verplicht *data protection impact assessment* en verantwoordingsinformatie, eerder zullen leiden tot meer papier dan betere gegevensbescherming. Data holders zouden in zijn visie meer dan nu een *mindset* moeten ontwikkelen die is geworteld in de grondbeginselen van gegevensbescherming, en niet in compliance met regels. Als een mogelijke oplossing ziet hij een terugkeer naar de geest van de onderliggende privacyprincipes zoals dataminimalisatie en gebruiksminimalisatie (zie tab 1), die ondernemingen zouden moeten incorporeren in hun governancerichtlijnen.
Het ligt buiten het kader van dit artikel een uitspraak te doen over de mate waarin de privacywetgeving succesvol is en de wijzigingen van de AVG een verbetering zullen betekenen. Waar we met nadruk wel op willen wijzen, is dat IT-auditors niet voorbij moeten gaan aan de potentiële tekortkomingen die wetten als de Wbp of de AVG in zich dragen om een adequate bescherming van persoonsgegevens voor elkaar te krijgen. Dat op zichzelf is al genoeg reden om bij privacy-aangelegenheden verder te kijken dan compliance alleen.

Adviezen en take-aways

De werkzaamheden die organisaties moeten uitvoeren om compliance met de AVG in 2018 te waarborgen, zullen een prominente plek op de privacy-agenda voor 2017 hebben. Privacyprofessionals, juristen, leveranciers van *privacy enhancing technologies*, en informatiebeveiligers spinnen daar garen bij. Maar ook de IT-auditor, als deskundige op het gebied van kwaliteitsvraagstukken in ICT, heeft een belangrijke rol te vervullen. Om dat te kunnen doen zou hij moeten uitgaan van (en in sommige gevallen teruggrijpen op) een meer holistisch privacybegrip, waarbij de geest van de bescherming van persoonsgegevens centraal staat en niet wordt overgeslagen ten faveure van de letter van de wet. In kader 2 hebben we een aanzet gegeven tot een aantal vragen die de IT-auditor hierbij zouden kunnen ondersteunen.

Het IT-auditberoep in Nederland heeft een lange en actieve geschiedenis als het gaat om het incorporeren van privacy in zijn kwaliteitsbeoordelende activiteiten. Daarvan getuigen onder andere de werkzaamheden van de Kennisgroep Privacy van NOREA, bijvoorbeeld de Privacy Impact Assessments (PIA's). NOREA zou een actieve en stimulerende rol moeten (blijven) vervullen in het creëren van concrete beoordelingskaders die meer omvatten dan compliance en informatiebeveiliging.

De 'lenzen' die we in dit artikel hebben besproken zijn niet meer dan een opzet voor een fundamentelere beoordeling van privacyvraagstukken. Concretisering en aanvulling daarvan zijn mogelijke onderwerpen voor verdere studie en bespreking.

Klik op deze link voor de onderbouwing.

Kader 2: Adviezen voor de IT-auditor

Laten we als voorbeeld de situatie nemen van een IT-auditor die als adviseur optreedt bij een data holder die een nieuwe soort verwerking of een wijziging in een bestaande verwerking van persoonsgegevens overweegt. Natuurlijk is het dan verleidelijk om meteen de Wbp of de AVG ter hand te nemen, de toelichting daarop van de Autoriteit Persoonsgegevens ernaast te leggen, en op basis van een toetsing daaraan een uitspraak te doen of de beoogde verwerking mag. Daarmee kan worden voldaan aan een verantwoording naar wetgever en toezichthouder, maar niet noodzakelijkerwijs ook naar data subjects of de maatschappij als geheel. Dat laatste zou ons inziens wel het doel van de betrokkenheid van de IT-auditor moeten zijn. In de geschetste situatie zou de IT-auditor de volgende vragen kunnen stellen om zijn toegevoegde waarde te vergroten.

1. Brengt de (nieuwe) verwerking een machtsverschuiving in de zin van Bambauer met zich mee? Is er sprake van fundamentele veranderingen in de toegang van belanghebbenden tot persoonsgegevens? Hiervan kan bijvoorbeeld sprake zijn als persoonsgegevens door de data holder worden gedeeld met andere partijen, ook al gebeurt dit volledig binnen de ruimte die de wet biedt. Spelen er – binnen een volgens de wet geautoriseerde verwerking – andere risico's zoals verlies van vertrouwen of zelfbeschikking, of uitsluiting aan de zijde van data subjects?
2. Wat is de algemene houding van deze data holder als het gaat om het verzamelen van persoonsgegevens? Zijn dataminimalisatie en gebruiksminimalisatie daadwerkelijk als governanceprincipes herkenbaar? Hebben de aspecten *predictability-manageability-disassociability* een plaats in het privacy-ontwerp?
3. Zijn dilemma's, belangen en belanghebbenden voldoende in kaart gebracht? Heeft er een analyse plaatsgevonden van wat de voorgestelde verwerking voor elk van die belanghebbenden in economische termen betekent? Is bij die analyse (dus ook) rekening gehouden met:
4. Risico's, kosten, maar ook opbrengsten en positieve effecten voor data subjects?
5. Opbrengsten, voordelen, maar ook risico's, kosten, en negatieve effecten voor de data holder?
6. Maatschappelijke effecten en het maatschappelijk belang (zie ook punt 1)?
7. Is de overweging niet alleen gefocust op de vraag 'hoe maximeren we als data holder het nut van de persoonsgegevens die we van een data subject in bewaring krijgen?' maar ook op 'hoe compenseren we de data subjects daarvoor? *What's in it for them?*' En kunnen we dit voldoende onderbouwen en overtuigend communiceren?
8. Is bij het voorstel tot (nieuwe) verwerking voldoende aandacht besteed aan overwegingen van proportionaliteit? Met andere woorden: staat de inbreuk op de belangen van de data subjects in verhouding tot het met de (nieuwe) verwerking te dienen doel?
9. Is bij het voorstel tot (nieuwe) verwerking voldoende aandacht besteed aan overwegingen van subsidiariteit? Met andere woorden: heeft de data holder onderzocht of er minder ingrijpende mogelijkheden zijn om hetzelfde verwerkingsdoel te bereiken, en is de conclusie dat dit niet plausibel of mogelijk is voldoende onderbouwd?
10. Kan de risico-afweging worden versterkt door het voorliggende privacyvraagstuk vanuit een aanvullende lens te benaderen (bijvoorbeeld op het gebied van ethiek of (nationale) veiligheid)?

Noten

[1] Gemakshalve beschouwen we datakwaliteit in dit artikel als onderdeel van het domein informatiebeveiliging.

Literatuur

[ACQI10] Acquisti, A., *The economics of personal data and the economics of privacy*. Heinz College Research, Carnegie Mellon University, 2010

[AUTO16a] Autoriteit Persoonsgegevens, *Europese Privacywetgeving*. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

[AUTO16b] Autoriteit Persoonsgegevens, *Jaarverslag 2015.* Den Haag, 2016.

[BAMB13] Bambauer, D., Privacy versus Security. Journal of Criminal Law and Criminology, vol. 103 issue 3, 2013.

[EURL] EUR-Lex, *Het recht van de Europese Unie, Bescherming Persoonsgegevens*. Zonder jaartal. http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=URISERV:l14012&from=NL

[KOOP14a] Koops, B-J., *Privacy, informatieveiligheid en een onzichtbare medaille.* In: S. Kok e.a. (red.), Informatieveiligheid, Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014.

[KOOP14b] Koops, B-J., *The trouble with European Data Protection Law*. International Data Privacy Law 4, 2014.

[NASA01] NASA, *Web Accessability Best Practices,* 2001.

[NIST17] National Institute of Standards and Technology, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. NIST Internal Report 8062, januari 2017.

[OVER16] *Uitvoeringswet Algemene Verordening Gegevensbescherming*. Op Overheid.nl. https://www.internetconsultatie.nl/uitvoeringswetavg

[STRA13] Strahilevitz, L. Towards a positive theory of privacy law. Coase-Sandor Institute for Law and Economics working paper nr. 637, University of Chicago, 2013.

[SWIR12] Swire, P. (ed.), *Foundations of Information Privacy and data protection*. IAPP, 2012.

[USTA12] Ustaran, E. (ed.), *European Privacy, law and practice for data protection professionals*. IAPP, 2012.

[WARR90] Warren, S. en L. Brandeis, *The right to privacy*. Harvard Law Review vol. 4 nr. 5, december 1890.

Ed Ridderbeekx en Suzanne Scheuller

Ed Ridderbeekx is werkzaam als zelfstandig IT-auditor en is lid van de redactie. Suzanne Scheuller is werkzaam als Privacy Officer bij ABN AMRO. Hiervoor heeft zij het Management Traineeship bij ABN AMRO gevolgd en is ze twee jaar bij Group Audit werkzaam geweest als IT-auditor. Zij schrijft dit op persoonlijke titel.