iBestuur

magazine

> Ancilla van de Leest: De overheid is niet te vertrouwen

> EPD in de herkansing

> GIBIT: gemeentelijke inkoopvoorwaarden

Special over hoe de overheid onze gegevens kan beschermen.

grip op privacy

Onafhankelijk kwartaalmagazine voor de iOverheid. Nummer 21, jaargang 7, januari 2017

Bij deze meld ik een datalek, dat ik bovendien niet dichten kan: de Belastingdienst heeft van mijn BSN mijn BTW-nummer gemaakt en ik ben bij wet verplicht om dat BTW-nummer her en der te publiceren samen met mijn NAW-gegevens, veelal in combinatie met mijn IBAN. Als de gemeente Amsterdam een dergelijke gegevenscombinatie per ongeluk – akkoord, drieduizendvoudig, maar toch – naar de verkeerde ontvanger verstuurt, moet die dat tenslotte ook melden bij de Autoriteit Persoonsgegevens (AP). Overheid en privacy, best ingewikkeld.

Deze meldplicht datalekken is de opmaat naar de Europese Algemene Verordening Gegevensbescherming (AVG) die nu al voor flink wat onrust zorgt binnen de burelen van de overheid. Niet in het minst omdat er iets tegennatuurlijks in zit: de verordening dwingt tot terughoudendheid met persoonsgegevens waar de efficiënte overheidsorganisatie het liefst zoveel mogelijk data verzamelt en combineert.

Het lijkt echter bijkans onmogelijk dat de overheid in mei 2018 volledig AVG-proof zal zijn. Bijvoorbeeld omdat de vereiste accountability – waar bevinden zich alle gegevens en wat gebeurt ermee – onhaalbaar is voor het gros van de gemeenten waar eindeloos veel kopieën van gegevensbestanden over evenzoveel afdelingen zwerven. Of omdat de noodzakelijke inhaalslag van de beveiliging blijft steken bij de halte ‘back-up en software-upgrade’. Of simpelweg omdat de bepalingen over de verwerking van persoonsgegevens in uiteenlopende wetten niet matchen! Niet alleen bij het inrichten van processen, maar ook bij het opstellen van wetten is ‘privacy by design’ een voorwaarde.

Daarnaast wringt de strikte doelbinding - en daarmee de controleerbaarheid - die de verordening oplegt met de huidige praktijk van creatief hergebruik van big data. Denk bijvoorbeeld aan de Belastingdienst en de snelwegfoto’s.

Naar verluidt was het toenmalig minister Opstelten die met een vooruitziende blik in Brussel voorstelde dat de draconische boetes waarin de AVG als sanctie voorziet, niet zouden gelden voor overheden. Dat wist u niet? Lees er artikel 83, lid 7 van de AVG op na: ‘Het is aan de lidstaten om in regels vast te leggen of boetes kunnen worden opgelegd aan overheidsorganisaties.’ Onlangs publiceerde het ministerie van VenJ het voorontwerp van de Uitvoeringswet AVG. Daarin is de mogelijkheid voor het opleggen van boetes aan overheden niet opgenomen. Zoals gezegd: overheid en privacy, best ingewikkeld!

Peter Lievense

i n d i t n u m m e r

Ancilla van de Leest:

‘De overheid is niet te vertrouwen’

Bij de Piratenpartij gaat privacy boven alles

Door **Bas Linders**
Beeld **Lex Draijer/De Beeldredaktie**

De Piratenpartij wil Edward Snowden politiek asiel geven, ethisch hacken belonen, rekeningrijden tegenhouden en meer rechercheurs in plaats van meer blauw op straat. Zolang die maar niet proberen om onze computers te hacken. Want privacy gaat boven alles!

Haar verschijning maakt dat Ancilla van de Leest, lijstaanvoerder van de Piratenpartij, in interviews vaker wordt gevraagd naar haar verleden als model dan naar haar politieke programma. In dat programma neemt privacy een centrale plaats in.

Is het digitaliseren van de overheidsdienstverlening nou een vooruitgang of juist een bedreiging voor de burgers?

“Ik vind dat digitalisering van overheidsdiensten een goede zaak is, maar je moet wel goed kijken hoe je het inricht. Op het moment dat heel veel experts roepen dat iets onverstandig is moet je als overheid niet zeggen: we doen het toch, want we moeten bij de tijd blijven. Zoals de digitalisering zich nu ontwikkelt, worden niet de mogelijkheden benut om mensen sneller en beter te informeren en inspraak te geven, maar stevenen we af op het inrichten van een massasurveillance-tool. Daarbij wordt alles wat iedereen doet opgeslagen en kunnen vervolgens profielen worden doorverkocht. Als dat de fundering wordt van de informatiesamenleving en het internet, dan loopt het niet goed met ons af.”

Wat moet er volgens jou gebeuren om die ontwikkeling tegen te gaan?

“Als je eenmaal systemen hebt geïmplementeerd wordt het heel lastig om daar nog op terug te komen op het moment dat ze niet goed werken. Dus volgens mij moeten we heel goed kijken hoe we dat aanpakken en inrichten. Op dit moment zie ik dat het uitrollen van de informatisering van de overheid niet zorgvuldig gebeurt. Daarom zou er een Ministerie van Digitale Infrastructuur moeten komen en een Staatssecretaris voor gegevensbescherming.

Alles wat de overheid doet moet gestoeld zijn op het waarborgen van de privacy van burgers. Op het moment dat burgerservicenummers of DigiD-codes naar de verkeerde mensen worden gestuurd – en dat is in Amsterdam voorgekomen – is dat dodelijk voor het vertrouwen in dat soort systemen. Je zadelt individuele burgers op met het risico op identiteitsfraude waar ze wellicht hun hele leven last van kunnen houden.''

Burgers komen ook in problemen omdat ze maar raak doen op internet en hun gegevens gewoon weggeven.

"Ik ben voor een grote mate van eigen verantwoordelijkheid, maar op het moment dat de overheid onzorgvuldig met persoonsgegevens omgaat en de burgers daarvan de dupe laat worden, is dat onacceptabel."

Is de overheid wel te vertrouwen?

"Nee, de overheid is niet te vertrouwen. Je kunt de overheid wél controleren en dat moeten we ook zeker doen. Daarom zijn we ook voor e-democracy. Het nu bestaande gat tussen besluiten en de uitvoering daarvan en de samenspraak daarover met de burger is veel te groot."

Waar is het volgens jou misgegaan?

"Het mooie van het oorspronkelijke internet was de decentrale opzet, terwijl het nu steeds meer het speelveld wordt van een paar grote wereldspelers als Google en Facebook. Die gaan steeds meer bepalen en voorschrijven hoe je internet moet gebruiken en zich bemoeien met de aard van de informatie die je zoekt of opvraagt. Als je vanuit Nederland googelt op Egypte krijg je iets heel anders te zien dan als je dat doet vanuit het Midden Oosten. In grote delen van Afrika denken mensen dat ze laagdrempelig internet hebben gekregen, terwijl ze in werkelijkheid te maken hebben met het platform van Facebook Zero."

Is Trump gekozen dankzij of ondanks internet?

"Ik denk wel dankzij, omdat de mainstream media een duidelijke voorkeur hadden voor Clinton. Dus als mensen alleen daar hun informatie hadden kunnen halen dan zouden ze wel voor Clinton hebben gekozen."

Ik zou dan zeggen: tel uit je winst met die informatie via internet, daar krijg je Trumps van.

"Hillary was ook geen goede kandidaat en ik denk dat internet dat heel zichtbaar heeft gemaakt."

Dankzij de 'customised' antwoorden die de mensen kregen op hun vragen op internet?

"Internet is niet meer de plek waar iedereen hetzelfde antwoord krijgt op dezelfde vraag."

Wat kan het Binnenhof daar nou aan doen?

"Netneutraliteit, dat is waar wij ons sterk voor maken. En ik vind dat Nederland niet genoeg weerstand biedt aan de Facebooks van deze wereld. België heeft bijvoorbeeld bezwaar gemaakt dat Facebook profielen maakt van niets vermoedende Belgen die niet eens een Facebook-account hebben. Vanuit Oostenrijk is met succes verzet aangetekend tegen de privacygevolgen van het Safe Harbour verdrag."

Nederland is als land vóór netneutraliteit en dat verzet vanuit België en Oostenrijk is succesvol vanwege een stelsel van Europese wetten. Zo slecht is het dus niet gesteld toch?

"Het is waar dat we op Europees niveau veel strengere privacywetten hebben dan in individuele landen, maar het is dan wel aan de overheid om te waarborgen dat die wetten ook worden nageleefd. De Europese privacyverordening die in 2018 van kracht wordt, zorgt ervoor dat bedrijven veel bewuster om moeten gaan met de gegevens van hun klanten en dat ze niet zomaar van alles mogen verzamelen. Dat is een goede zaak en een stap in de goede richting. Volgens mij is de taak van de overheid om de macht van bedrijven een beetje in toom te houden. In de digitale samenleving houdt dat in dat je bedrijven moet wijzen op hun verantwoordelijkheid om zorgvuldig met hun persoonsgegevens om te gaan."

Overheden werken toch ook heel succesvol samen met techbedrijven ?

"Was het niet Mussolini die zei: 'fascism is the merger between corporate and state'."

Zullen kiezers de Piratenpartij ooit zien als wat anders dan een verzameling hacktivisten en tegenstanders van intellectueel eigendom?

"Wij zijn geen 'one-issue' partij. De digitalisering van de samenleving heeft invloed op bijna elk aspect van het dagelijks leven. Op de zorg, op de werkgelegenheid, op de veiligheid, op het onderwijs, op de voedselvoorziening, op de wijze waarop de financiële sector werkt. We leven in een tijd van 'massasurveillance', waarbij wijzelf en al onze financiële transacties in de gaten worden gehouden. Een tijd waarin je niet meer anoniem kunt reizen en waarin je elke dag moet 'betalen' met je persoonlijke gegevens om gebruik te kunnen maken van zogenaamde gratis diensten. Wij zijn dus een hele brede partij die zich zorgen maakt over allerlei maatschappelijke ontwikkelingen. We vinden dat informatisering er moet zijn in het belang van de mensen en niet om alleen maar het belang te dienen van een handvol internationale bedrijven die alles en iedereen in hun greep krijgen."

Is dat niet een erg somber wereldbeeld? Is het einde der tijden echt in zicht? Je hebt toch ook nog wel een paar idealen?

"Als je niks doet wordt het nog erger, maar ik ben best wel optimistisch. Je ziet nu al dat je met erg weinig moeite toch heel veel kunt bereiken als het gaat om het bewust maken van mensen. Inmiddels is privacy echt een onderwerp dat regelmatig aan bod komt in de media. De EU-landen moeten in mei 2018 de privacyverordening invoeren die bedrijven verplicht om zorgvuldig met hun klantgegevens om te gaan. De toenemende robotisering zorgt voor een nieuw maatschappelijk debat over de noodzaak van een basisinkomen. Er is discussie over de vraag of de politie er wel goed aan doet om WhatsApp van Facebook aan te bevelen als gereedschap voor buurtpreventie. Dat politie en justitie willen kunnen inbreken in de computers van burgers is gelukkig ook niet zo maar een hamerstuk meer in het parlement. Als het lukt om in de Tweede Kamer te komen wil ik het voortdurend over dit soort zaken hebben."

Privacy is een mensenrecht en dat is niet voor niets

Wat moet er op de prioriteitenlijst van de beleidsmakers bij de overheid?

"Ik vind dat beleidsmakers in Den Haag zich zorgen moeten maken over de groeiende digitale macht van de bancaire sector. Die zijn druk bezig om het gebruik van contant geld onmogelijk te maken en mensen straks alleen nog maar de mogelijkheid te geven om te pinnen. Op het moment dat we dat doen dan wordt dus al het betaalverkeer digitaal bijgehouden, geïndexeerd en tot het einde der tijden opgeslagen. Dat zijn een heleboel persoonsgegevens. Banken hebben ook al aangegeven dat ze heel veel interesse hebben om die gegevens over het betaalgedrag van hun klanten weer door te verkopen. Dat is een ontwikkeling waar ik me grote zorgen om maak en die zorgen zouden beleidsmakers ook moeten hebben. Verder is het Landelijk Schakelpunt – het voormalige Elektronisch Patienten Dossier – waarbij de verzekeraars steeds meer toegang tot medische gegevens krijgen, iets wat op de schop moet. Ik ben het eens met de mensen in de gezondheidszorg die dat een gevaar voor de volksgezondheid vinden. Mensen moeten ervan verzekerd kunnen zijn dat wat zij met hun dokter bespreken ook privé blijft."

De Piratenpartij kan deze onderwerpen toch niet claimen. Andere politieke partijen hebben in hun programma's vergelijkbare thema's. En wat doet Sophie in 't Veld van D66 in Europa volgens jou niet goed?

"Sophie zit in het Europees parlement en ik ga nu voor de landelijke politiek. Ook daar is iemand nodig."

Kun je je doelen niet beter bereiken met activiteiten buiten de Tweede Kamer in plaats van het kluitjesvoetbal voor een kamerzeteltje?

"Als ik zie wat de Partij voor de Dieren voor elkaar heeft gekregen met twee zeteltjes dan zie ik heel veel mogelijkheden".

Marianne Thieme sluit haar bijdragen in de Tweede Kamer altijd af met een oproep om een eind te maken aan de bio-industrie. Wat wordt – als het ervan komt – jouw afsluiter?

"Daar ben ik nog op aan het broeden, maar ik denk iets in de trant van: 'privacy is een mensenrecht en dat is niet voor niets!'."

Versus

Privacy versus aanbestedingen

Veel overheden nemen het niet zo nauw met de bescherming van uw en mijn persoonsgegevens. Zo rommelen talloze gemeenten maar wat aan met gegevens die zij van hun burgers vragen, bijvoorbeeld met het oog op maatschappelijke ondersteuning. Ook de technische beveiliging van IT-systemen blijkt niet zelden ver benedenmaats. In een publieke cultuur waarin kostenbeheersing het veelal wint van andere waarden, sneuvelen belangen rondom een zorgvuldige omgang met gegevens al snel. Anderzijds: het oerwoud van privacywetgeving is inmiddels verworden tot voer voor superspecialisten.

Een bron van problemen is dat medewerkers van de afdeling inkoop en aanbestedingen nauwelijks overleg hebben met hun collega's die verantwoordelijk zijn voor privacy. Gevolg: een rommeltje bij de inkoop van bijvoorbeeld cloud- of hostingdiensten. We zien dat onder meer bij uitbesteding in de sfeer van het zaakgericht werken, een ontwikkeling die al enige tijd speelt bij lagere overheden.

Wat is het probleem? De privacywet in ons land verlangt bikkelhard dat de opdrachtgever een zogeheten 'bewerkerscontract' met de cloud- of hostingprovider sluit. Zo'n contract moet de nodige waarborgen bevatten voor de bescherming van de persoonsgegevens, zoals toereikende afspraken over beveiligingsmaatregelen, vertrouwelijkheid en auditing. Zonder een bewerkerscontract schend je als overheid elementaire spelregels op het gebied van privacy. Deze wettelijke verplichting bestaat weliswaar sinds 2001, maar veel opdrachtgevers lapten die tot voor kort steevast aan hun laars. Door de komst – per begin 2016 – van nieuwe wetgeving over datalekken is de belangstelling voor bewerkerscontracten echter plotsklap enorm toegenomen. Wil je als overheidsinstantie netjes jouw datalekken aan de Autoriteit Persoonsgegevens en de gedupeerde burgers kunnen melden, dan moet je daarover goede afspraken hebben met de cloud- of hostingprovider die je hebt ingeschakeld. De kans bestaat immers dat het datalek zich voordoet in het datacenter van de provider. Het is daarom niet vreemd dat overheden de laatste maanden op grote schaal bewerkerscontracten aan hun zittende IT-providers ter ondertekening hebben voorgelegd.

Dat wringt met het aanbestedingsrecht. Het is in de regel een aanbestedingsrechtelijke doodzonde als een reeds lopende contractuele verhouding wordt opengebroken met nieuwe afspraken. Het aanbestedingsrecht gaat er immers vanuit dat tevoren - dat wil zeggen in de gepubliceerde aanbestedingsstukken - alle voorwaarden en condities waaronder een overheidsopdracht wordt vergeven, duidelijk en precies zijn opgenomen. Daar past dus niet bij dat achteraf nog eens nieuwe afspraken bij de IT-provider naar binnen worden geschoven. Ook geen bewerkerscontracten.

En dat plaatst overheden in een onoplosbare klem: kies je ervoor het privacy-recht langer te schenden door geen bewerkerscontract met de provider te sluiten? Of schend je de beginselen van het aanbestedingsrecht door juist wel een bewerkerscontract voor te leggen? Aan u als overheidsinstantie de keuze....

Mr. Peter van Schelven
Juridisch adviseur inzake ICT

De nieuwste Jouw Gemeente Mijn Gemeente-serie gaat over MijnOverheid

Van fysiek naar digitaal loket

Meine Hofman, beleidsmedewerker ICT bij de gemeente Urk.

Dirk Visser, gegevensmanager gemeente Urk.

Welke gemeente wil nou niet leren van een andere gemeente? Helemaal als die gemeente al iets heeft gedaan wat jij nog niet hebt gedaan, maar wel zou willen doen. Om deze reden is het inspiratieplatform 'Jouw Gemeente Mijn Gemeente' in het leven geroepen. Het nieuwste onderwerp waar we induiken? MijnOverheid!

Voor steeds meer zaken hoef je niet meer naar het stadhuis, maar kun je hetzelfde ook digitaal afhandelen. Een belangrijke bouwsteen van de digitale overheid is MijnOverheid, de website waarop burgers overheidszaken met gemeenten en de Rijksoverheid kunnen regelen. In de nieuwe videoserie van 'Jouw Gemeente Mijn Gemeente' gaan we kijken wat de voor- en nadelen zijn van de overstap naar MijnOverheid.

Kiezen voor digitale communicatie

Want het gaat snel: alle communicatie met consumenten/burgers wordt steeds meer digitaal. Waar het eerst vooral banken en retailbedrijven waren die overstapten naar digitale communicatie, zie je inmiddels dat ook de Rijks- en gemeentelijke overheid steeds meer voor online communicatie gaan. Zeker ook sinds de komst van MijnOverheid. De mogelijkheden van dat platform zijn ook legio: nu worden vooral de belastingaanslagen via MijnOverheid verstuurd, maar het zal niet lang duren voordat overal in Nederland ook paspoorten en vergunningen via het platform kunnen worden aangevraagd. En dit zijn maar twee voorbeelden van de vele mogelijkheden.

Wat komt kijken bij de overstap?

Maar voor het zover is, moeten gemeenten de belangrijke keuze maken: stappen ze wel over op MijnOverheid? En zo ja, wat komt kijken bij de overstap naar digitale communicatie met de burger? Daar gaan we in de nieuwe serie 'Jouw Gemeente Mijn Gemeente' achter komen. In een aflevering laten we Meine Hofman, beleidsmedewerker ICT bij de gemeente Urk, op bezoek gaan bij Els de Swart, invorderingsambtenaar bij de gemeente Horst a/d Maas. De eerste gemeente is al overgestapt, de gemeente Urk wil begin volgend jaar overstappen op MijnOverheid. De benodigde techniek is daar al aanwezig, alleen de organisatie moet nog worden uitgewerkt.

Van elkaar leren: ambtenaren van Urk en Horst a/d Maas gaan bij elkaar op bezoek

Omgekeerd neemt Dirk Visser, gegevensmanager bij de gemeente Urk, een kijkje in de keuken van de gemeente Horst a/d Maas. Hij sprak daar af met Saner Janssen, teammanager klantcontact. Dirk Visser vroeg zich onder andere af wat de overstap naar MijnOverheid heeft betekend voor de inwoners en hoe zij de inwoners op de hoogte hebben gesteld van de veranderingen.

Aan de slag

Na de bezoeken is de conclusie van Meine Hofman en Dirk Visser dat er nog wat werk te verrichten valt voordat de Urkers vóór eind februari 2017 gebruik kunnen maken van de digitale berichtenbox. Er zijn nog wel een aantal stappen te zetten binnen de gemeente Urk.

Benieuwd naar welke stappen? Wil je alle antwoorden en uitdagingen weten die komen kijken bij de implementatie van MijnOverheid? Bekijk dan de korte documentaire waarin het bezoek van Urk aan Horst a/d Maas is vastgelegd. Naast de videoserie is er op het platform nog meer inspiratie te vinden in de vorm van persoonlijke blogs van de deelnemers en een stappenplan voor implementatie. Bezoek dus snel www.jouwgemeentemijngemeente.nl om alles te weten te komen over de impact van MijnOverheid voor een gemeente.

Over 'Jouw Gemeente Mijn Gemeente'

PinkRoccade Local Government lanceert 'Jouw Gemeente Mijn Gemeente', een inspiratieplatform waarbij ervaringen van IT-talenten van verschillende gemeenten op het gebied van digitalisering worden gedeeld. Het platform bestaat uit een videoreeks, waarbij IT'ers worden uitgedaagd om een dag inspiratie op te doen bij een andere gemeente, en daarnaast blogposts van deelnemende gemeenten, handige tools en whitepapers.

Met het platform Jouw Gemeente Mijn Gemeente biedt PrinkRoccade Local Government IT'ers de kans om een kijkje te nemen in de digitale keuken van een andere gemeente, en zo kennis op te doen voor de eigen organisatie. De afgelopen maanden zijn de onderwerpen Cloud en Centraal Debiteurenbeheer behandeld. Meer informatie:

http://www.jouwgemeentemijngemeenten.nl

Veilig publieke diensten leveren met tablets

Beeld: Pixabay

Met beveiligde tablets werken in het onderwijs en met leerlingmanagementsystemen.

Burgers, bedrijven en overheid kunnen op vele manieren contact maken en in contact blijven. Elk van deze manieren heeft zijn eigen voor- en nadelen: portals zijn relatief goedkoop, maar bieden niet altijd voldoende interactie. Direct contact is duurder, maar persoonlijker en dus effectiever. Het gaat erom een goede balans te vinden tussen kosten, functionaliteit en impact.

"Het uitgangspunt van dienstverlening zou toch moeten zijn: hoe kan de burger of een bedrijf op de meest prettige manier met je in contact komen. Daar heb je medewerkers voor nodig die mobiel zijn, zowel in plaats als tijd. Die kunnen problemen oplossen op de plek waar dat nodig is én die kunnen daarnaast efficiënt hun tijd indelen. Hiervoor moeten ze zo worden uitgerust dat zij dat werk ook op elke plek optimaal kunnen verrichten", zegt Joris Schut, Innovation Strategist bij Capgemini .

Capgemini levert daar met het Integraal Mobiel Platform (IMOP) een bijdrage aan. Schut: "De basis van IMOP is een managed tablet. Medewerkers worden voor een vast bedrag per maand uitgerust met een van afstand beheerde beveiligde tabletcomputer, een leaseconstructie dus. 'Managed' betekent onder andere dat alleen aan vooraf goedgekeurde functionaliteiten en applicaties toegang wordt verleend. Het is ook mogelijk gebruik te beperken tot alleen in de zakelijke omgeving of de werkomgeving te voorzien van een eigen look and feel. Uiteraard kunnen gebruikers op afstand worden ondersteund. Tenslotte is ook een pick-up&return-service beschikbaar en kan de organisatie worden begeleid bij de inrichting van de afgeschermde omgeving."

De IMOP-dienst biedt dienstverleners de mogelijkheid om medewerkers effectief mobiel te laten werken. Dankzij de met internet verbonden tablet kunnen medewerkers naar de plek gaan waar burgers en bedrijven hen nodig hebben. Ze kunnen dan ter plekke informatie opzoeken of opvragen en de zaken regelen waarom wordt gevraagd. Dienstverleners zijn hierdoor in staat om sneller situaties in te schatten, deze te delen met anderen en, indien nodig, acties te ondernemen.

De introductie van mobiele hulpmiddelen vraagt en leidt onvermijdelijk tot organisatorische en culturele veranderingen. Om overheden te helpen die omslag te maken biedt Capgemini de nodige ondersteuning. Hierbij valt te denken aan het opstellen van business cases, coaching van medewerkers en het opnieuw inrichten van strategie en bijbehorende processen.

Toepassingsgebieden voor mobiel werken

Binnen het overheidsdomein zijn talloze toepassingsgebieden te bedenken waar mobiel werken bestaande processen kan versimpelen of dienstverlening efficiënter kan maken. Innovation Strategist Jeroen de Wit: "Denk aan de politieagent op straat of bijvoorbeeld aan inspectiediensten. Daarnaast zijn er programma's beschikbaar voor het onderwijsdomein die het gepersonaliseerd leren op tablets mogelijk maakt. Ten slotte is er een 'Out of the Box' leerlingmanagementsysteem beschikbaar waarmee organisaties een eigen digitale leeromgeving kunnen bouwen."

"Allemaal toepassingsgebieden die door de unieke propositie van IMOP kunnen worden ondersteund en waarbij kosten, functionaliteit en impact met elkaar in balans zijn", concludeert De Wit.

Voor informatie over het Integrated Mobiel Platform kunt u contact opnemen met Joris Schut via joris.schut@capgemini.com, Jeroen de Wit via jeroen.de.wit@capgemini.com of via de website nl.capgemini.nl/imop.

Joris Schut; Innovation Strategist

Jeroen de Wit; Innovation Strategist

EPD in de herkansing

Het EPD is dood, leve het EPD. In oktober werd de Wet Cliëntenrechten bij elektronische verwerking van gegevens aangenomen. Is dat de doodsteek voor de privacy, een overwinning voor de patiënt of een interessant businessmodel?

Door **Petra Pronk**
Beeld **Shutterstock**

Het leek zo vanzelfsprekend. Stel dat je tijdens een dagje uit bewusteloos in een ziekenhuis belandt. Dan is het wel handig als de behandelend arts je dossier kan inzien zodat je geen medicijnen krijgt waar je allergisch voor bent. Met dergelijke voordelen voor ogen werd de wet Elektronisch Patiëntendossier (EPD) ontwikkeld. Die moest medische gegevensuitwisseling mogelijk maken tussen zorgverleners, onder toezicht van de Rijksoverheid (toen: VWS).

In maart 2009 nam de Tweede Kamer de wet EPD aan; in april 2011 verwierp de Eerste Kamer dit voorstel unaniem. Hoofdbezwaar: de privacy zou onvoldoende gewaarborgd zijn.

Daarna werd het ingewikkeld. De motie Mulder voorkwam eind 2011 dat de infrastructuur van het EPD bij het grof vuil kwam. Een doorstart moest toch mogelijk zijn als zorgkoepels een private vorm aan het EPD gaven. Minister Schippers beaamde dit volmondig. Het voorstel ging terug naar de tekentafel.

Zorgverzekeraars, patiëntenverenigingen en koepels van zorgaanbieders ontwikkelden een nieuw voorstel waarbij het Landelijk SchakelPunt (LSP) onder regie kwam van de Vereniging van Zorgaanbieders Voor Zorgcommunicatie (VZVZ). Op 1 juli 2014 nam de Tweede Kamer de Wet Cliëntenrechten bij elektronische verwerking van gegevens aan. De Eerste Kamer volgde op 4 oktober 2016.

Deze ‘parapluwet’ regelt de aanpas-

sing op onderdelen van enkele reeds bestaande wetten: Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens). Deze wetten samen regelen de randvoorwaarden voor elektronische uitwisseling van medische persoonsgegevens, zoals het toestemmingsprincipe voor het delen van informatie, het recht op inzage in het eigen dossier en de beveiliging.

Toestemmingsprincipe

De nieuwe wet scherpt de voorwaarden aan waaronder patiëntengegevens mogen worden gedeeld: dat mag alleen via gespecificeerde toestemming. Omdat de ICT-systemen van de zorgverleners daar niet op zijn ingesteld, krijgt het veld drie jaar de tijd om dat te regelen. Tot die tijd wordt er nog gewoon met generieke toestemming gewerkt.

Huisarts in ruste en EPD-deskundige Wim Jongejan vindt dat van de gekke. “We tolereren dus met z’n allen generieke toestemming, terwijl iedereen het erover eens was dat zoiets niet wenselijk is. Dat is te zot voor woorden. Deze wet is echt een wangedrocht. Bovendien is er geen enkele garantie dat wat nu niet lukt, over drie jaar wel kan! Maar het is het bekende verhaal van de olietanker: niemand durft hem te stoppen.”

PGO

De nieuwe wet regelt ook dat patiënten expliciet het recht krijgen op digitale toegang tot hun gegevens via een Persoonlijke Gezondheids Omgeving (PGO). De patiënt krijgt daarmee de beschikking over onderdelen van zijn dossier en mag dit zelfstandig beheren, aanvullen en delen met derden. De Patiëntenfederatie Nederland is daar blij mee, maar veel zorgverleners maken zich zorgen.

Een PGO is een interessante optie voor mondige, zelfbewuste burgers, maar hoeveel zijn er daarvan? Professionals in alle hoeken van de zorg hebben sinds de invoering van de Wet Maatschappelijke Ondersteuning (WMO) al te maken met gemeenten die vaak op hoge toon inzage eisen in medische gegevens. Ze zijn bang dat die praktijk onder de nieuwe wet hand over hand zal toenemen.

Huisarts Pascale Hendriks uit Spaarndam kan erover meepraten. Eén van haar patiënten kreeg van de gemeenteambtenaar die over haar uitkering ging te horen dat zij psychologische hulp moest zoeken. Vervolgens belde de ambtenaar Hendriks op om te checken of deze vrouw inderdaad een verzoek voor doorverwijzing had gedaan. De huisarts liet de ambtenaar weten dat die het recht niet heeft om dit soort informatie op te vragen omdat die onder het beroepsgeheim valt. Maar de ambtenaar liet zich niet afschepen en dreigde met korten op de uitkering.

Ook collega-huisartsen worden belaagd door partijen met interesse in medische data, van de thuiszorgambtenaar tot de leverancier van incontinentiemateriaal, van de zorgverzekeraar tot de verzuimmedewerker. Tot nu toe konden zorgverleners hun patiënten daartegen in bescherming nemen, maar onder de nieuwe wet kan dat niet meer. “Patiënten krijgen het mes op de keel om inzage te geven in hun dossier. Nee zeggen is bijna niet mogelijk, want dan krijgen ze bepaalde voorzieningen niet. Dat is een complete uitholling van de privacy en oneigenlijk gebruik van het dossier”, aldus een boze huisarts.

Positief

Niet iedereen is zo somber. Wim Hodes, directeur-bestuurder van GERRIT, een regionale samenwerkingsorganisatie van zorgaanbieders op het gebied van informatie-uitwisseling en ICT, benadrukt de versterking van de informatiepositie van de patiënt. “Het is belangrijk dat zorgaanbieders beschikken over een compleet en actueel dossier. In de praktijk is dat echter vaak niet het geval, omdat aanvullende informatie ontbreekt die de patiënt zélf heeft.”

GERRIT startte in september samen met VZVZ en zorgaanbieders in Friesland een pilotproject met het Intelligent Persoonlijk Medicatiedossier (IPMD). Daarin kunnen patiënten inloggen in het Landelijk Schakelpunt (LSP) en zo toegang krijgen tot de eigen medicatiegegevens. Die gegevens kunnen vervolgens worden opgehaald in de app Medische Kluis op de eigen mobiel, waarna de patiënt ze kan bewerken en terugsturen.

Voor de gegevensbeveiliging ging GERRIT in zee met de Rijksdienst voor het Wegverkeer (RDW): “De RDW heeft goede papieren als het gaat om digitale beveiliging. Bij het overschrijven van auto’s is het cruciaal dat je zeker weet dat de juiste persoon ‘aan de knoppen zit’. Datzelfde geldt voor de overdracht van medische gegevens.”

Hodes betreurt dat de aandacht voor privacy afleidt van waar het echt om gaat: patiëntveiligheid. “Als ik bloedverdunners gebruik wil ik graag dat de specialist in het dorp waar ik op vakantie ben dat ook weet. Wij maken ons druk over privacy, maar het lijkt mij minstens zo belangrijk om ons druk te maken over de vraag of de informatie in een patiëntendossier wel juist en compleet genoeg is, want door onjuiste en gebrekkige informatie gaan er dingen serieus mis.” Hodes hoopt na de evaluatie begin volgend jaar de handen op elkaar te krijgen voor het verder opschalen van het project.

Cardiologie on demand

Dat mensen voortaan hun eigen dossier kunnen beheren, biedt kansen aan bedrijven die iets doen met medische data. Toen het wetsvoorstel in 2011 werd afgestemd, stond big data-analyse nog in de kinderschoenen, maar inmiddels is dit een serieus element in de discussie en een kans voor ondernemende professionals. Neem Janneke Wittekoek, cardioloog bij HeartLife Klinieken. Zij is een groot voorstander van ‘cardiologie on demand’ en van het delen van gezondheidsdata tussen dokter en patiënt. “In de reguliere zorg liep ik altijd achter de feiten aan, maar dankzij de techniek kan ik nu heel gericht mijn tijd besteden aan mensen die mij nodig hebben.”

Wittekoek werkt met een applicatie waarbij patiënten via een beveiligde verbinding gegevens over hun bloeddruk, hartslag, gewicht, medicatie, bijwerkingen en klachten naar een portaal kunnen sturen, waar de informatie vervolgens via een algoritme wordt omgezet in codes: rood (urgent), oranje (minder urgent) of groen (niet urgent). “Dankzij die data heb ik mensen direct bij de staart als er een probleem is. Ik kijk ’s morgens in mijn computer of we mensen hebben die rood scoren en daar bellen we dan achteraan. Zo hoef ik mijn tijd niet te verdoen met mensen met wie het goed gaat. Dat is efficiënt en effectief.”

Voor Wittekoek is dit nog maar het begin. Zo is ze ook bezig met het ontwikkelen van een app met een digitaal kaartensysteem waarbij patiënten elke dag een kaart toegestuurd krijgen met informatie over gezondheid, variërend van recepten tot oefeningen. “Wij noemen dat nudge-kaarten. Nudging is een belangrijk begrip in de preventieve cardiologie: iemand een duwtje geven in de goede richting door gewenst gedrag aantrekkelijk te maken. Het is nu nog eenrichtingsverkeer, maar het is de bedoeling dat we in de toekomst ook kaarten van patiënten terugkrijgen waar getallen opstaan over hun bloeddruk en cholesterol. ICT kan eraan bijdragen dat het voorkómen van hart- en vaatziekten echt een ‘joint effort’ wordt van patiënt en dokter.”

Big data

Grote bedrijven als Philips zien ook nieuwe business in gezondheidsgegevens. Big data-analyse vormt daar een onderdeel van. Het koppelen van grote hoeveelheden data maakt patronen inzichtelijk en leidt uiteindelijk tot betere behandeling, is het idee. Zo presenteerde Philips onlangs Illumeo, een systeem dat via kunstmatige intelligentie radiologen helpt met het verwerken van grote hoeveelheden medische informatie, onder andere uit patiëntendossiers. Philips richt zich ook op ‘fall detecting technology’. In de Verenigde Staten levert het bedrijf al een apparaatje dat ouderen bij zich kunnen dragen en dat alarm slaat bij een val. Dat apparaat is ‘getraind’ op basis van gegevens over onder andere het bewegingsgedrag van de eigenaar.

Kansen en bedreigingen

De nieuwe wet maakt allerlei nieuwe initiatieven mogelijk. Dat biedt kansen, maar brengt ook bedreigingen met zich mee. Het delen van medisch data staat op gespannen voet met het bewaken van de privacy. Zo stelde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dit jaar dat ‘big data’ weliswaar een bijdrage kan leveren aan de kwaliteit en doelmatigheid van de zorgverlening, maar ook het gevaar met zich meebrengt van inbreuk op de privacy en diefstal van gegevens.

Zo maakt de Wet Marktordening Gezondheidszorg het mogelijk dat zorgverzekeraars rechtstreeks en zonder toestemming van de patiënt medische gegevens kunnen opvragen bij een vermoeden van fraude, iets waar de verzekeraars volgens de VVAA geregeld misbruik van maken. De VVAA liet daarom Spong Advocaten dit wetsvoorstel juridisch toetsen. De conclusie was niet mals: de wet is in strijd is met het Europees Verdrag voor de Rechten van de Mens (EVRM). Volgens het EVRM weegt een principieel belang zoals de privacy van patiënten zwaarder dan een financieel belang als fraude.

Verzet kwam ook van de kant van privacy-organisatie Bits of Freedom. Die gaf Minister Schippers bij de uitreiking van de Big Brother Award de publieksprijs voor diezelfde wet, omdat het medisch beroepsgeheim door die wet verder zou afbrokkelen.

En dan hebben we het nog niet over crimineel misbruik van medische gegevens gehad. Volgens Intel Security richten cybercriminelen zich steeds vaker op diefstal van medische gegevens. Die gegevens zouden in het zwarte circuit inmiddels vijf keer zoveel waard zijn als creditcardgegevens.

We tolereren generieke toestemming, terwijl iedereen dat onwenselijk vindt

Samen bouwen aan een infrastructuur voor iedereen

We hebben al veel bouwstenen voor een sterke e-overheid. Er ontbreken echter een aantal essentiële elementen die deze bouwstenen met elkaar verbinden tot een krachtig geheel.

Een groep leidinggevenden vanuit de e-overheid publiceerde onlangs een voorstel op de website van iBestuur. Zij waren op bezoek in Estland en vertaalden hun bevindingen in dit voorstel voor de nieuwe regeerperiode. Larissa Zegveld, directeur van KING, maakte deel uit van deze Estlanddelegatie en schreef mee aan het voorstel. “Wat we zien is dat de Nederlandse overheid de bouwstenen heeft voor een sterke e-overheid, maar er ontbreken een aantal essentiële elementen die deze bouwstenen samensmeden tot een krachtig geheel.” De groep pleit voor het maken van één overheidsbreed gedragen visie op de e-overheid die leidt tot verplicht stellende afspraken. “Het ontbreekt in Nederland niet aan visie, maar we hebben er nogal veel. Iedereen heeft zijn eigen digitale agenda, ook wij als VNG en KING. Wij raden aan om te komen tot één visie die voor de hele overheid geldt en waar iedereen in samenhang aan kan werken. Daarbij hebben we een organisatie nodig die de noodzakelijke bevoegdheden krijgt om overheidsbreed te sturen dat deze afspraken daadwerkelijk worden nagekomen.”

Verbinden wat er al is

De digicommissaris heeft de afgelopen jaren hard gewerkt om meer samenhang aan te brengen en duidelijke afspraken te maken over de financiering en governance van de generieke digitale infrastructuur, de basis van de e-overheid, stelt Zegveld. “Nu is het tijd om de e-overheid zodanig te versterken dat we gaan werken als één efficiënte overheid.” Het voorstel van de Estlanddelegatie bevat een aantal punten om dit te bereiken. Volgens Zegveld is er veel te leren van het Baltische land, al is de situatie daar anders dan in Nederland. Zo kon Estland min of meer vanaf nul beginnen, terwijl Nederland al een uitgebreide infrastructuur heeft. “Daarom benadrukken we het belang van het leggen van verbindingen tussen wat er al is. Juist door te benutten wat we al hebben, kunnen we snel grote stappen maken.” De Estlanddelegatie stelt onder meer voor om verder bouwen aan een stelsel van generieke bouwstenen, een uitbreiding van de GDI met onder meer portalen, kanalen voor gegevensuitwisseling en online identificatiemiddelen.

Samen organiseren

Het pleidooi om veel meer samen te doen haakt aan bij een trend die al bestaat onder gemeenten. Op de Buitengewone Algemene Ledenvergadering van de VNG afgelopen november stemden gemeenten met grote meerderheid voor een aanpak van samen organiseren, in lijn met de bestaande Digitale Agenda 2020. VNG en KING ondersteunen gemeenten daarbij. Gezamenlijk inkopen doen gemeenten al: de eerste gezamenlijke inkoop ging over mobiele datacommunicatie en de inkoop voor vaste telefonie loopt. Zo zullen er meer volgen, zegt Zegveld: “Alles wat voor gemeenten een commodity is, kunnen we gezamenlijk inkopen.”

Ook op het gebied van gemeentelijke producten en diensten worden nu grote stappen gezet. De webdiensten waarmee mensen een verhuizing online doorgeven en de webdienst waarmee begrafenisondernemers digitaal een overlijden melden, zijn inmiddels gegund aan Decos. Dat bedrijf gaat voor deze diensten de e-formulieren en de achterliggende technologie maken. Dat resulteert in twee landelijke webdiensten die alle gemeenten kunnen gebruiken. In 2017 volgen er meer gemeentelijke diensten die op deze manier aanbesteed en vervolgens gebouwd gaan worden. Zoals het aanvragen van uittreksels. Een andere generieke voorziening is Govroam, waarmee ambtenaren veilig kunnen inloggen op wifi-netwerken van andere deelnemende overheidsorganisaties. KING spant zich er voor in dat alle gemeenten zich hierbij aansluiten, zodat er een landelijk dekkend Govroamnetwerk komt.

> Het ontbreekt in Nederland niet aan visie, maar we hebben er nogal veel

Leefwereld wordt leidend

Dit is allemaal werk onder de motorkap van de e-overheid, zegt Zegveld. Het is noodzakelijk dat het gebeurt, maar de Estlanddelegatie pleit voor een bredere visie. “Wat ons opviel in Estland is de open en positieve houding ten opzichte van digitalisering. Men ziet het echt als een kans voor nieuwe en betere dienstverlening.” Daarom pleit de delegatie onder meer voor innovatie als norm bij de ontwikkeling van de digitale overheid. Met andere woorden: digitaliseer niet alleen bestaande dienstverlening, maar innoveer de dienstverlening. Zegveld geeft een voorbeeld uit de gemeentelijke praktijk: “Als we de webdienst voor uittreksels collectief gaan oppakken, dan zullen we onderzoeken of we deze dienst zo kunnen vormgeven dat deze niet meer vraagt ‘welk uittreksel heeft u nodig?’, maar dat aan de hand van de levensgebeurtenis van de inwoner wordt aangegeven welke uittreksels nodig zijn.”

Een goed werkende e-overheid is echter meer dan dienstverlening die zich voegt naar de leefwereld van inwoners en ondernemers. “Uiteindelijk moeten al onze inspanningen leiden tot één efficient werkende overheid, die optimaal aansluit bij de samenleving. Als een onderdeel van die samenleving, aangehaakt op een infrastructuur die van die hele samenleving is. En die overheid, markt en inwoners gebruiken voor het vergroten van hun welvaart en hun welzijn. We hebben in Estland gezien hoe dit kan werken. Dat moet in Nederland ook mogelijk zijn.”

Beeld: Dreamslitme

Eén weg in het woud van inlogmiddelen

DigiD, iDIN, Idensys... er komen steeds meer manieren bij om in te loggen bij de overheid. Dat is goed voor de dienstverlening, want burgers en ondernemers kunnen de methode kiezen die ze het prettigst vinden. Maar websites moeten wel al die inlogmiddelen gaan ondersteunen.

Als burgers en ondernemers snel en veilig kunnen inloggen, dan zullen zij eerder gebruikmaken van de online dienstverlening van de overheid. Dat is essentieel om de digitale doelstellingen van de overheid, zoals Digitaal 2017, te behalen. Wat daarbij enorm zou helpen is een solide én gebruiksvriendelijk stelsel voor online identificatie en authenticatie. Daar wordt dan ook volop aan gebouwd.

De bestaande voorzieningen met DigiD (voor burgers) en eHerkenning (voor ondernemers) worden uitgebreid. Dat doen de private sector en de overheid samen. “We groeien toe naar een hybride stelsel, waarin diverse middelen voor identificatie en authenticatie naast elkaar zullen bestaan. Dat betekent dat websites meerdere inlogmiddelen moeten gaan ondersteunen”, zegt Johan de Jong, thoughtleader Digital Transformation bij CGI. De ministeries van BZK en EZ werken samen met de private sector aan middelen voor online identificatie en authenticatie, onder de naam Idensys. De banken gaan hun eigen oplossing, genaamd iDIN, ter beschikking stellen aan derde partijen. Daar kan de overheid in haar dienstverlening dan ook gebruik van maken. Met iDIN logt een burger met zijn pasje en identifier van zijn bank in bij een overheidsdienst, waarna de bank aan de overheid bevestigt dat deze burger inderdaad is wie hij zegt te zijn. Daarna kan deze burger online diensten afnemen via de overheidswebsite.

Keuze

Martijn Kaag, directeur van Connectis, benadrukt dat burgers en bedrijven eerder van online overheidsdienstverlening gebruik zullen maken als zij de keuze hebben uit verschillende inlogmiddelen. “Inloggen met je bankpas via iDIN of telefoon via Idensys is makkelijk en veilig. Je gebruikt je bankpas en mobiel bijna dagelijks, veel vaker dan je DigiD. Voor iDIN en Idensys geldt bovendien dat het verificatieproces veel veiliger is. Je krijgt je account pas na het tonen van je paspoort, terwijl voor DigiD het ontvangen van een brief al voldoende is.” Meerdere middelen om in te loggen maakt het gebruik van online dienstverlening laagdrempeliger en klantvriendelijker, stellen Kaag en De Jong. En het verlaagt de kosten, want online dienstverlening is goedkoper dan dienstverlening via telefoon en balie.

De middelen voor online identificatie en authenticatie zullen in de toekomst alleen maar verder worden uitgebreid, bijvoorbeeld met methoden om in te loggen met je smartphone of je social media profiel. De Jong: “We gaan toe naar een situatie waarin mensen op de websites die ze bezoeken kunnen kiezen hoe ze willen inloggen. Een beetje zoals het nu gaat met betalen op webwinkels. Daar kun je vaak kiezen uit meerdere opties. Zoals betalen via iDeal, creditcard of acceptgiro.”

Bring your own ID

Het is overigens niet alleen klantvriendelijk om meerdere inlogmethoden te ondersteunen; het is straks zelfs wettelijk vereist. Dat vraagt nogal wat van de infrastructuur die onder websites ligt. Connectis en CGI richten zich in hun samenwerkingsverband op deze uitdaging. Samen ontwikkelden ze Bring Your Own ID (BYOID): een oplossing die het mogelijk maakt om met alle bestaande middelen veilig in te loggen.

Connectis is één van de grootste identity-bemiddelaars in Nederland. Hun infrastructuur wordt ingezet voor 80 procent van alle transacties met eHerkenning en verwerkt miljoenen DigiD transacties. BYOID gebruikt deze infrastructuur om het inloggen via meerdere middelen te ondersteunen. De Jong: “Het kost veel tijd en geld om zelf op je eigen websites de functionaliteit te bouwen en te onderhouden die verschillende inlogmethoden ondersteunt. Daarom bieden wij BYOID aan als een service. Alle identificatiemiddelen die binnen de EU beschikbaar zijn werken in deze oplossing. Er is één koppeling tussen de website van de organisatie en deze oplossing.”

Solide oplossingen voor identificatie en authenticatie helpen Nederland om kansen in digitalisering te benutten. Dat gaat om veel meer dan overheidsdienstverlening. Ook e-health zal bijvoorbeeld een grotere vlucht nemen als mensen dergelijke toepassingen veilig kunnen gebruiken.

Er wordt hard gewerkt aan een stelsel van publieke en private veilige middelen voor identificatie en authenticatie. De Jong: “Met BYOID zorgen we dat de overheid daar nu al op voorbereid is. Zo maakt de overheid een veilige sprong vooruit met de digitalisering van haar dienstverlening.”

Met je DigiD inloggen bij de Franse overheid

Eind 2018 moet het voor burgers en bedrijven uit de hele Europese Unie mogelijk zijn om met hun eigen nationale inlogmiddel in te loggen bij overheidsinstanties binnen de EU. Zodat bijvoorbeeld iemand uit Frankrijk met de Franse versie van DigiD kan inloggen bij het CJIB om een openstaande boete te bekijken. Dit is vastgelegd in de Europese Verordening elektronische identiteiten en vertrouwensdiensten (eIDAS). In 2016 zijn door Connectis 81 gemeenten gekoppeld aan eIDAS. Medio 2017 koppelen het Centraal Justitieel Incassobureau (CJIB), de uitvoeringsorganisatie van het ministerie van volksgezondheid, welzijn en sport (CIBG) en de Rijksdienst voor Ondernemend Nederland (RVO) aan.

De gemeente Nijmegen wilde bij de geplande aanpak van enkele verkeersknelpunten hard maken dat de luchtkwaliteit daarbij niet zou verslechteren. Dit vormde het startpunt voor het opzetten van een burger-sensor-netwerk. Overheid én inwoners kunnen daarbij over dezelfde data beschikken.

Niels van de Graaf

Beter inzicht in de luchtkwaliteit van Nijmegen

Het bedrijfsleven en gemeenten hebben op de Nationale Klimaattop in Rotterdam afspraken gemaakt over de terugdringing van de CO_2-uitstoot. Dit zijn fantastische afspraken en hopelijk gaat het hen allemaal lukken. Maar hoe weet een gemeente of bedrijf dat ze op de goede weg zijn?

Meten is weten in zo'n geval. De gemeente Nijmegen heeft daartoe een uniek burger-sensor-netwerk ontwikkeld. De basis daarvan ligt in 2014 toen de gemeente een samenwerking startte met onder andere Radboud Universiteit om beter inzicht te krijgen in de CO_2-uitstoot en andere luchtkwaliteitindicatoren (NO_2, CO, CO_2, O_3). De betrokkenheid van de universiteit had ook als doelstelling een betere communicatie met en hogere betrokkenheid van inwoners te realiseren.

De directe aanleiding was de geplande aanpak van een aantal verkeersknelpunten. De gemeente wilde hard maken dat de luchtkwaliteit met de komst van nieuwe wegen niet zou verslechteren. Paul Geurts, informatie-architect bij de gemeente, las tijdens zijn vakantie over de plannen. Hij las in de digitale krant op zijn tablet ook welk budget de gemeente had voorzien om die luchtkwaliteitmetingen gedurende een aantal jaren uit te voeren. Dat kon slimmer, beter en goedkoper, dacht hij. Terug van zijn vakantie vatte hij direct de koe bij de hoorns en ging in gesprek met collega's en diverse instanties. Dit was het startpunt van het Smart Emission project.

Smart Emission Project

De essentie van het 'Smart Emission' project is dat inwoners helpen met het in kaart brengen van luchtkwaliteit, geluid, trillingen en meteorologische indicatoren. Omgekeerd krijgen inwoners realtime toegang tot alle data.

In het project wordt onderzocht welke (geo)infrastructuur er nodig is om de data van het burger-sensor-netwerk te verwerken. Bovendien wordt bekeken hoe deze data zo kan worden gevisualiseerd dat onderzoekers en bewoners die kunnen raadplegen en daarover communiceren. Aansluiting kon worden gezocht met het subsidietraject Maps4society en samen met de Radboud Universiteit is een project opgesteld voor een low-cost sensornetwerk met participatie van de burger. De medewerking van de RU zorgde direct voor wetenschappelijk toezicht op het project.

In het project worden ook zaken meegenomen die niet passen bij reguliere economische afwegingen, maar die wel effect kunnen hebben op de gezondheid van een stad en haar inwoners (zogeheten 'externiteiten'). Ten slotte zijn de planologen van de Radboud Universiteit geïnteresseerd welke potentie dit wederzijds gebruik van open data biedt voor de samenwerking tussen burgers en lokale overheid.

Binnen Europa zijn vele enigszins verwante 'bottom-up' processen gestrand. Maar in Nijmegen niet. Dat is vooral dankzij de beschikbaarheid van goedkope en betrouwbare sensoren en van geavanceerde visualisatie. Het project bleef betaalbaar omdat kon worden volstaan met goedkope sensoren. Die bleken verrassend betrouwbaar, zoals een vergelijking met de RIVM-sensoren duidelijk maakte. (RIVM zelf heeft de sensoren ook getest.) Bovendien konden de meetresultaten dankzij een kalibratieformule worden gecorrigeerd ten opzichte van professionele sensoren van het RIVM.

Overzichtelijk dashboard

Ook de visualisatie van de meetgegevens heeft veel aandacht gekregen. Daarvoor kwam men bij Imagem uit. De Smart M.App technologie van het bedrijf maakt het mogelijk om allerlei soorten data en bronnen eenvoudig met elkaar te verbinden en deze op interactieve en dynamische wijze te visualiseren.

Imagem heeft voor dit project een dashboard (Smart Emission M.App) gerealiseerd dat realtime in één overzicht de luchtkwaliteit inzichtelijk maakt. Door eenvoudige metertjes te gebruiken worden de meetwaarden direct begrepen. Voor gebruikers die dieper in de meetgegevens willen duiken zijn er aparte tabjes gemaakt waarin trends en ontwikkelingen van de diverse parameters geanalyseerd kunnen worden. Het RIVM is kennisinhoudelijk betrokken.

Stand van zaken

Het project is gestart. Verschillende burgers hebben zich al aangemeld om mee te doen met de monitoring. Bij hen zijn inmiddels sensoren geplaatst.

Dit alles is niet onopgemerkt gebleven. Nijmegen heeft de Slimste Stad prijs gewonnen in de categorie 'De Slimste Binnenstad van Nederland'. De overwegingen van de jury zijn onder anderen: directe impact op de kwaliteit van leven, klaar voor een succesvolle uitrol in andere gemeentes, aanzet tot de cultuuromslag bij de gemeente Nijmegen voor de samenwerking met burgers.

Het is de intentie van Nijmegen om de Smart Emission M.App verder te ontwikkelen tot een volwassen en volledig productierijpe oplossing. Die zal dan de komende jaren in de lucht worden gehouden. Daarna zal de oplossing geïntegreerd moeten worden binnen de gemeentelijke processen. Meer onderzoek zal gedaan worden naar de participatie van de burger. Het draait namelijk niet alleen om Smart City maar ook om Smart Citizens, de burger aan de knoppen. De gemeente zoekt ook naar verbreding zodat een community gerealiseerd kan worden.
Andere gemeenten kunnen nu ook aansluiten en de luchtkwaliteit in de eigen gemeente monitoren.

Le Grand Frère

In veel landen staat de democratie onder druk. Onder de noemer bescherming van de nationale veiligheid of de strijd tegen terreur worden grondrechten soms fors beperkt, waaronder het recht op privacy.

Zo ook in Frankrijk. Daar is al een jaar de noodtoestand van kracht en naar verwachting zal die nog minstens een half jaar worden verlengd. Die noodtoestand geeft de overheid buitengewone bevoegdheden en beperkt de rechterlijke macht. Overigens bleek dat de geheime diensten al sinds 2008 op grote schaal zonder enige wettelijke basis internet- en telefoonverkeer aftappen. In 2015 werden nieuwe wetten aangenomen die deze illegale praktijken legaliseren. Er is een uitzondering gemaakt voor Franse parlementariërs, maar niet voor het Europees Parlement dat elke maand in Straatsburg vergadert. Dus vallen de Europarlementariërs mogelijkerwijs onder de massa surveillance.

Parlementariërs moeten in alle vrijheid de regering kunnen controleren, niet de regering de parlementariërs. Die omkering is een bedreiging voor de democratie. Journalisten, advocaten en belangenorganisaties maar ook parlementariërs moeten vrijelijk hun werk kunnen doen. Zij zullen zich wellicht twee keer bedenken voordat ze politieke gevoeligheden aan het licht brengen of diepgaand onderzoek doen. Het zogenaamde ‘chilling effect’ van massa surveillance, waardoor bewakers van de democratie aan zelfcensuur gaan doen. Daarnaast kunnen machthebbers informatie ook misbruiken.

D66 pleit er al jaren voor dat afluisteren alleen op gerichte wijze gebeurt en op basis van een verdenking. We spreken ons hard uit tegen de zogenoemde sleepnetmethode. Door middel van steeds meer omvattende surveillance manoeuvreren we in de richting van een Orwelliaanse staat.

Houdt de Franse overheid mij in de gaten? Gezien mijn kritische houding ten opzichte van de Franse regering valt het niet uit te sluiten. Daarom heb ik bij de Franse toezichthouder een verzoek ingediend om uit te zoeken of ik ben afgeluisterd; en zo ja, of dat binnen de reikwijdte van de nieuwe Franse wetgeving en de Europese wettelijke kaders valt.

De Toezichthouder reageerde pas na de deadline en stelde in vage termen dat hij niets onwettigs had kunnen vaststellen. Daarop heb ik een klacht ingediend bij de Franse Conseil d’Etat. Daarin stel ik dat de Franse wet voor de sleepnetmethode niet in lijn is met het Europese Handvest voor de Grondrechten. En dat het ontbreken van een beroepsvoorziening, waarmee burgers een klacht kunnen indienen, in strijd is met de Conventie voor de Rechten van de Mens. Wellicht volgt er een beroepszaak voor het EU Hof in Luxemburg, of het Mensenrechten hof in Straatsburg.

De alomtegenwoordige, spiedende Big Brother uit Orwells 1984 was fictie, laten we dat vooral zo houden.

Sophie in ’t Veld
Lid van het Europees Parlement voor D66

De informatiesamenleving stelt ons voor complexe vraagstukken. Hoe we daarmee omgaan bepaalt hoe we onze toekomstige samenleving vormgeven en de rol van de overheid daarin. Dat vraagt om een dialoog waarin we tot nieuwe inzichten kunnen komen.

Informatiesamenleving van de toekomst vraagt om dialoog

Herriët Heersink, ICTU en Roxane Daniels, beleidsmedewerker informatiebeleid bij BZK.

Zullen iOverheid en iSamenleving straks niet een geheel nieuwe onderlinge verhouding hebben? “Combineer de netwerksamenleving met de iSamenleving en je weet dat we in staat moeten zijn om in hoog tempo en met een grote groep stakeholders oplossingen te bedenken voor moeilijke vraagstukken”, zegt Roxane Daniels, beleidsmedewerker informatiebeleid bij BZK. Daarom heeft BZK het initiatief genomen om een dialoog te starten over de iSamenleving. Met een diverse groep stakeholders het gesprek voeren om grip te krijgen op dat brede begrip iSamenleving. “Vanuit het idee dat we de ontwikkeling van de samenleving immers gezamenlijk vorm geven. En om een antwoord te kunnen formuleren op de vraag hoe we die ‘iSamenleving’ ervaren.”

Op 25 en 27 oktober startte de dialoog met zo’n vijftig mensen. Twee middagen waarin nieuwe perspectieven en inzichten ontstonden. En waar een basis is gelegd voor vervolgsessies.

De Nederlandse samenleving is in hoge mate gedigitaliseerd. Dat geldt ook voor de overheid. Die sterke digitalisering en inzet van technologie verandert onze samenleving en de verhoudingen tussen groepen in die samenleving. Privacy heeft een andere lading gekregen, opsporing verloopt op een andere manier, we communiceren anders met elkaar. Vroeger stond bijna iedereen graag in het telefoonboek met huisadres en al, nu houden we dat misschien liever privé. We profiteren van online diensten, maar willen graag een echt persoon spreken als we een moeilijke vraag hebben.

BZK stelt een nieuwe beleidsagenda op voor de komende jaren. Daar zal de focus niet alleen liggen op de digitalisering van de overheid, maar ook op de ontwikkeling van de informatiesamenleving en de rol die de overheid in die context te spelen heeft.

Vraagstukken en antwoorden moeten daarbij niet alleen uit de eigen gelederen komen, maar juist uit de samenleving, in gesprek óók met ‘unusual suspects’ en vanuit verschillende perspectieven. “Het is niet meer van deze tijd om te veronderstellen dat de meest interessante kennis wel bij de grote instellingen en bedrijven te vinden is. De samenwerking met organisaties zoals het Pakhuis de Regâh*.*, een onafhankelijk stadsplatform, is daarom waardevol.”

Casuïstiek

Waarom zouden de dialoog-bijeenkomst andere inzichten opleveren?

Aanbevelingen

De Dialoog Informatiesamenleving levert ook aanbevelingen aan voor bijvoorbeeld de I-Agenda van de toekomst. Alle sessies zijn openbaar toegankelijk en de uitkomsten zijn voor iedereen beschikbaar. De verzamelde uitspraken uit de dialoogbijeenkomsten (oktober 2016) zijn gegroepeerd en hebben vooralsnog tot vijf aanbevelingen geleid die als basis voor verdere discussie kunnen dienen:

- **Verleg de focus in beleid van technologie (ICT) naar de mens.**
- **Benut gedragswetenschappelijke inzichten, analyseer behoeftes voorbij zichtbaar gedrag en pas toe op de verhouding tussen overheid en iSamenleving.**
- **Investeer in het probleemoplossend vermogen van inwoners en ambtenaren. Observeer, analyseer, experimenteer, maak keuzes en leer.**
- **Versterk de tweestromenaanpak binnen de overheid. Zorg dat de overheid toegankelijk en aanspreekbaar is.**
- **Zet wet- en regelgeving slim in, toon voorbeeldgedrag en hou de dialoog over de iSamenleving gaande.**

Daniëls: “Op het eerste gezicht lijken dit geen nieuwe inzichten. Maar als je ze goed doordenkt hebben ze misschien wel grote gevolgen. Wanneer we eens niet over de ICT zouden praten maar over de mens en het gebruik van die ICT, zouden we dan andere keuzen maken? Het is het overdenken waard.”

‘Onder de Haagse stolp vandaan komen bevrijdt’

Arre Zuurmond, ombudsman van Amsterdam, ziet duidelijk voordelen aan de aanpak van de Dialoog Informatiesamenleving. “Gewoon ergens in een wijk gaan zitten en een paar mensen uit die wijk erbij betrekken, dat werkt toch wel goed. Ik had een gesprek met Cis, een kunstenares die veel met kinderen werkt. Je merkte aan haar dat ze het wel heel veel jargon vond, maar niet schroomde om dat aan de orde te stellen. Dat hielp enorm. Er zaten ook gewone mensen van vlees en bloed die wijkgerichte ervaringen inbrachten en daardoor een nuchterheid en een leefwereld die op zich al goed was.”

Voor beleidsambtenaren en andere overheidsmensen is het volgens Zuurmond helemaal niet zo moeilijk eens uit hun eigen abstracties te stappen. “Dat gebeurt dan vanzelf. Die mensen uit de ivoren torens zijn ook gewoon mensen van vlees en bloed die opa’s en oma’s en neven en nichten hebben die in een andere situatie leven. Een echte dialoog vindt men uiteindelijk ook wel fijner dan die brave gesprekken op departementen. Onder de Haagse stolp vandaan komen bevrijdt eigenlijk iedereen, gek genoeg.”

Er kwamen voor Zuurmond een paar dominante inzichten naar boven over hoe het met de oprukkende digitalisering nog enigszins menselijk te houden is. “Misschien moet je veel meer een overheid van twee snelheden maken: de simpele gevallen drastisch digitaliseren en de ruimte die daardoor vrijkomt gebruiken voor de langzame overheid die echt aandacht voor je heeft. Een ander antwoord is dat je voor kwetsbare burgers veel meer integrale dienstverlening moet organiseren waarbij één accountmanager een burger in alle vraagstukken helpt in plaats van – wat nu gebeurt – dat je een burger verwijst naar zeven loketten die elk afzonderlijk op maximale efficiency zijn ingericht.”

Herriët Heersink, die vanuit ICTU samen met BZK de dialoog organiseert: “Wat we bewust doen is aan de hand van een casus vragen stellen aan de mensen.” De eerste bijeenkomst ging uit van de kwestie Chantal, het meisje dat slachtoffer was van een door haar ex op Facebook gepubliceerde sexvideo. “Dat is wat nu werkelijk in onze samenleving gebeurt.”

Daniels: “We vertrekken vanuit een incident als dit, en kijken vervolgens naar de onderliggende waarden. Wat vinden we belangrijk in onze samenleving en hoe willen we met elkaar omgaan?”

De tweede bijeenkomst werd ingeleid door Arre Zuurmond, ombudsman van Amsterdam en omstreken. (Zie kader.) “Hij ziet van dichtbij wat de impact is van digitalisering op de samenleving en wat de rol van de overheid hierin is. Essentieel is het beginnen met de voeten op de vloer: dít is wat er nu al gebeurt en wie heeft hierin welke rol? Iedere keer kan er in zo’n bijeenkomst dus aan de hand van een stukje werkelijkheid worden gepraat.”

Heersink vindt de vraag gerechtvaardigd of het nog wel correct is te praten over de ‘iSamenleving’. “Eigenlijk praat je gewoon over de veranderende samenleving. Maar als je de ‘i’ weglaat is de kans groot dat de aandacht verdwijnt voor wat die i teweeg brengt.”

Collectief gesprek

Daniels: “Er bleek bij de bijeenkomsten niet altijd eenstemmigheid over de te kiezen richting, maar dat is ook niet erg. Er zullen altijd verschillen van mening blijven bestaan. Het gaat erom dat we met elkaar in gesprek blijven en elkaars perspectieven onderzoeken, uitvinden waar we het wel met elkaar over eens zijn. En zo bij wijze van spreken voorvechters van vernieuwing en zwaar bevochten rechten met elkaar in contact brengen. De overheid is ook aan het zoeken naar welke rol ze hierin kan pakken en heeft behoefte om sneller te kunnen reageren. En om beter te kunnen omgaan met die hoge dynamiek van de iSamenleving. Aan de dialoogtafels komt dit vraagstuk in een relatief korte tijd aan de orde.”

De dialoog vindt niet alleen in fysieke bijeenkomsten plaats maar ook in de vorm van columns en publicaties, theaterstukken en foto’s. Zo dragen allerlei partijen op verschillende manieren bij aan het gesprek over hoe de iSamenleving eruit moet komen te zien. Op 12 januari gaat de dialoog verder met een bijeenkomst over democratie en digitalisering.

Je gaat het pas zien als je het doorhebt

Ruud Böhmer (ICTU) en Friso van der Meulen (TNO)

Eigenlijk is het verbazingwekkend dat organisaties op informatiegebied iedere keer weer hun hoop vestigen op de nieuwste technologieën en tools. Verbazingwekkend, omdat ondanks het feit dat veel medewerkers deze tools omarmen, er iets vreemds aan de hand is. Medewerkers klagen dat het steeds lastiger is om de juiste informatie te vinden die ze voor hun werk nodig hebben, terwijl organisaties steeds meer moeite hebben hun informatiehuishouding op orde te krijgen.

Professionals, ook binnen de overheid, zijn nog steeds veel tijd kwijt met niet-productieve ICT-activiteiten. Ze zoeken bijvoorbeeld naar informatie die eigenlijk onder handbereik zou moeten zijn, besteden tijd aan documentenbeheer, richten samenwerkingsruimten in en leveren managementinformatie aan uit andere systemen. En het aantal projecten en programma’s gericht op het op orde krijgen van de informatiehuishouding is onveranderlijk groot.

Meer van hetzelfde

We moeten ons dus afvragen hoe effectief en efficiënt de gebruikelijke manier van ondersteuning door ICT is. Want ondanks de inzet van nieuwe technologie hebben de oplossingen vaak een hoog meer-van-hetzelfde gehalte: een portal vervangt de desktop, de cloud de netwerkschijven en cases de dossiers. Maar het blijft lastig om de juiste informatie op het juiste moment, tegen minimale inspanning beschikbaar te hebben. Waarom is dit een probleem? Niet alleen is steeds meer werk complex en kennisintensief, maar ook worden hogere eisen gesteld aan efficiency en productiviteit. De noodzaak is dus groot om dat werk optimaal te ondersteunen en extra (ICT-) beheerstaken te vermijden. Dat gaat niet lukken als we oude ontwerpparadigma’s gebruiken om nieuwe technologie in te zetten.

Het is hoog tijd voor een andere benadering van de informatievoorziening voor de ondersteuning van professionals. We hebben oplossingen nodig die medewerkers van nu daadwerkelijk in hun werk ondersteunen, onnodig systeemwerk voorkomen en de weg openen naar significante efficiencywinst.

Hoe dan wel?

Op het gebied van organisatie-ontwerp wordt al jarenlang gestudeerd op en geëxperimenteerd met nieuwe organisatievormen. In het boek ‘Het Nieuwe Organiseren’ maken Herman Kuipers en Pierre van Amelsvoort inzichtelijk hoe de aard van het werk door de jaren heen is veranderd en benoemen ze de noodzaak voor een andere, flexibelere werkorganisatie. De ontwerpprincipes die daar worden gehanteerd geven ons inziens richting aan een ander type informatievoorziening, door ons Informatie Ondersteund Werken (IOW) genoemd. Het IOW-concept biedt een oplossing die daadwerkelijk ondersteunt en tegelijkertijd de informatiehuishouding van de organisatie op orde brengt.

Niet de ICT, maar de volledige werkcontext van de professional staat hierbij centraal. Dit leidt tot volstrekt andere inzichten op de inrichting van informatievoorziening, maar dat zie je pas als je het doorhebt. En daar willen we u natuurlijk graag bij helpen.

Binnenkort meer informatie over dit onderwerp op de website van ICTU www.ictu.nl.

GIBIT moet gemeente betere opdrachtgever maken

Op eigen voorwaarden

Inkoopvoorwaarden kunnen de relatie opdrachtgever-leverancier verhelderen en verbeteren. Na 'Elias' en berichten over ontevreden gemeenten geen overbodige luxe. Gemeenten streven nu met eigen inkoopvoorwaarden naar helderheid in hun verhouding tot de markt. Wordt het beter? Niet iedereen is overtuigd.

Door **Peter Mom**
Beeld **Marijn van Bekkum**

'Communicatie' paste niet zo goed in de afkorting. Het werd GIBIT: Gemeentelijke Inkoopvoorwaarden bij IT. Op 8 december heeft het VNG-bestuur, daartoe geadviseerd door de VNG-commissie Dienstverlening en Informatiebeleid, GIBIT formeel vastgesteld.

Inkoopvoorwaarden bestaan toch al? Zeker, maar de lokale overheid kan met deze Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT) niet altijd uit de voeten. Dat maakte een verkenning duidelijk die KING voorjaar 2015 in opdracht van de VNG en op aandringen van de Viag en de Gebruikersvereniging Centric uitvoerde naar de voorwaarden die gemeenten bij hun ICT-inkoop hanteren. Meest gebruikt werden algemene inkoopvoorwaarden van de eigen gemeente, gevolgd door leveringsvoorwaarden van de huisleverancier. Pas op plaats drie volgde ARBIT, waarbij wel opgemerkt moet worden dat gemeenten geregeld voor hun meest gebruikte algemene voorwaarden uit ARBIT putten.

Peter Klaver en Jeroen Schuuring waren bij KING verantwoordelijk voor de verkenning en de mede daarop gebaseerde totstandkoming van specifiek gemeentelijke voorwaarden. Zij stellen dat ARBIT minder goed bruikbaar is om conformiteit aan standaarden af te dwingen. Daaraan hebben gemeenten juist behoefte. Voor samenwerkingsverbanden, bij de vorming waarvan licenties moeten overgaan van afzonderlijke gemeenten naar een collectief, biedt ARBIT evenmin soelaas. Derde manco: de gerichtheid van ARBIT op systeemontwikkeling. Lokale overheden willen doorgaans standaardsoftware in plaats van maatwerkprogrammatuur.

Opdrachtgeverschap

Het opstellen van nieuwe voorwaarden hebben Klaver en Schuuring enthousiast aangevat nadat de VNG-ledenvergadering vorig jaar zomer bijna unaniem de Digitale Agenda 2020 omarmde en versterking van het gemeentelijk ICT-opdrachtgeverschap tot speerpunt maakte. Inkoopvoorwaarden worden geacht daaraan bij te dragen. Daartoe is de volgorde zoals gehanteerd in de (als basis genomen) ARBIT gewijzigd en de levenscyclus van een product gevolgd. De diverse stadia zijn vrij uitvoerig behandeld, zodat inkopers bij deugdelijke GIBIT-implementatie alle mogelijke inkoopaspecten onder hun aandacht gebracht zien.

GIBIT kwam tot stand met input vanuit een werkgroep met informatiemanagers, inkopers en juristen van vijftien gemeenten, en mensen van de Viag en de Gebruikersverenigingen Centric en PinkRoccade. Ook was er een klankbordgroep met bedrijven. Leveranciers die met een product in KING's Softwarecatalogus staan, zo'n 160, konden zich aanmelden. Dat leverde elf geïnteresseerden op, waaronder Centric en PinkRoccade, de twee grootste en nogal eens object van gemeentelijk ongenoegen. Oogmerk was niet, leggen Klaver en Schuuring uit, met die bedrijven tot overeenstemming te komen. Ze konden suggesties doen en aangeven hoe gemeentelijke ideeën zouden vallen dan wel of deze überhaupt toepasbaar zouden zijn.

Concept

Begin augustus lag de concept-GIBIT er en kregen gemeenten, leveranciers en koepelorganisaties een uitnodiging voor een 'brede consultatie'. Die leverde 95 commentaren op. Bijna tweederde was afkomstig uit gemeentelijke kring, zowat een kwart kwam van marktpartijen.

Waar bedrijven mogen meepraten, maar niet meebeslissen, ligt het voor de hand dat ze niet staan te juichen over het resultaat. Maar PinkRoccade heeft op het moment van navraag nog geen definitief standpunt. Volgens directeur Michiel Uijting gaat het bedrijf dat medio december bepalen. Wel wil hij kwijt dat hij de PinkRoccade-inbreng in de klankbordgroep 'te weinig ziet terugkomen in de eindversie'.

Ook Centric is gereserveerd. De scope van de inkoopvoorwaarden is veel breder en ze zijn ook behoorlijk gedetailleerd. "Nu levert een aanbesteding steeds minimaal dertig vragen en opmerkingen op. Dat zal aanzienlijk groeien", zegt commercieel manager Pierro Baas. Grotere gedetailleerdheid impliceert meer leveranciersverplichtingen. Dat zou tot hogere prijzen kunnen leiden, meent Baas.

Brancheorganisatie Nederland ICT was niet gevraagd voor de klankbordgroep. Jammer, vindt jurist Sylvia Huydecoper, die de branchereactie op het GIBIT-concept ook graag zag als het begin van een dialoog om 'tot een voor alle betrokkenen werkbare set te komen'. Dat VNG/KING de consultatie zo niet had gedacht, is een 'gemiste kans'. Ook zij wijst op de grote mate van detaillering. Daardoor is GIBIT niet flexibel, stelt ze. Steen des aanstoots is voorts de verdeling van risico's over opdrachtgever en -nemer. "Risico's zijn disproportioneel bij de markt gelegd", zegt Huydecoper. "Dat kan bedrijven ontmoedigen om op opdrachten in te schrijven." Na vaststelling van GIBIT door het VNG-bestuur zal Nederland ICT haar leden gaan voorlichten over hoe er zodanig mee om te gaan dat ze minimaal risico lopen.

Verscheidenheid

Jurist Ruud Leether, oud-legal counsel van het ministerie van Veiligheid en Justitie en de man achter de rijksvoorwaarden ARBIT, ziet GIBIT eveneens ten nadele van de markt uitpakken. (Zie het kader.) Hij vindt dat waar KING pretendeert tot uniformering van inkoopvoorwaarden te komen, de verscheidenheid met GIBIT juist toeneemt.

Dat de gemeentevoorwaarden, zeggen de opstellers, van ARBIT afwijken is niet vreemd na de conclusie uit de verkenning dat rijksvoorwaarden niet voldoen en gemeenten op hun specifieke situatie toegesneden voorwaarden willen. Klaver en Schuuring wijzen er ook op dat wijzigingen zijn aangebracht als gevolg van signalen uit de bedrijven-klankbordgroep en de brede consultatie. Zo zijn bepalingen over intellectuele eigendom aangepast (die berust van pakketsoftware bij de leverancier en van maatwerk bij de opdrachtgever) en is bij de verdeling van risico en aansprakelijkheid in sommige situaties wederkerigheid ingevoerd (als een project sneeft door een fout bij de opdrachtgever, kan het bedrijf daarvoor niet verantwoordelijk worden gehouden).

Risicoverdeling hangt af van de soort opdracht. Met een softwarepakket van de plank, dat reeds bij tig gemeenten draait, loopt een aanbieder minder risico dan met een innovatieve maatwerkexercitie, die zich nog moet bewijzen. KING's GIBIT-duo stelt dat dit niet in één clausule valt te vatten en van geval

tot geval in het uiteindelijke contract geregeld kan worden. Het verlangt bij elke aanbesteding en elk inkoopproces opnieuw beoordeling.

Risicoverdeling

Evenwicht. Dat is ook een rode draad in het relaas van Arjen Gerritsen, als bestuurder bij de materie betrokken. Hij is burgemeester van Almelo en lid van de VNG-commissie Dienstverlening en Informatiebeleid. “Je kunt het niet eenzijdig opleggen en zeggen: daar moet iedereen het mee doen. We hebben steeds gezegd dat we het bedrijfsleven erbij moeten betrekken. Maar het blijft een product van en voor gemeenten. Het zijn inkoopvoorwaarden, geen standaardcontracten. Anderzijds, als de markt GIBIT niet kan absorberen, kan het ook niet werken.”

Dat GIBIT te weinig flexibel en te gedetailleerd zou zijn, daarover is Gerritsen ‘niet helemaal zonder begrip’. Maar: “Doelders is, beantwoordt hij met: “Goed. Maar gemeenten moeten hun opdrachtgeverschap versterken. De eisen aan gemeentelijke ICT worden steeds hoger. Qua integriteit van infrastructuren, qua samenwerking… dan wil je goed spul hebben. GIBIT veronderstelt niet dat nu geen goed spul wordt geleverd. Of dat gemeenten het zelf moeten doen. Nee, daarvan ben ik geen voorstander. Er is een markt. Ik wil geen brood bakken, ik wil brood kopen.”

Ondersteuning

KING bereidt zich intussen voor om gemeenten te ondersteunen bij het gebruik van GIBIT. Ze zijn autonoom en bepalen zelf of en zo ja hoe ze de voorwaarden aanwenden. Met ‘kennissessies’ wil KING ze maximaal aan GIBIT krijgen.

Hoe vinden zij eigenlijk het resultaat? VNG en KING zijn natuurlijk content. Maar Viag en GV Centric, allebei eveneens gemeenteclubs, die bovendien mede de stoot gaven tot gemeentelijke inkoopvoorwaarden? Ligt er nu wat hun voor ogen stond?

“Het is een mooie uitkomst die gemeenten erg behulpzaam is bij het aangaan van contracten”, zegt Viag-voorzitter Arend van Beek. “Iedereen kan er zijn voordeel mee doen, ook leveranciers. Rechten en plichten zijn eenduidig beschreven.”

Terughoudendheid

Voor Gebruikersvereniging Centric ligt het een tikje anders, laat secretaris Wicher Venema weten. Centric-klanten vinden GIBIT op zich een goede ontwikkeling, maar wensen meer draagvlak aan leverancierskant. Nu dat bij Centric ontbreekt gaat de GV GIBIT als basis gebruiken voor een gesprek met het bedrijf om tot een wel voor beide partijen aanvaardbare regeling te komen, zoals ze ook nu modelovereenkomsten kennen. Leden die GIBIT toepassen, roept de GV op ervaringen te melden als input voor dat overleg met Centric.

Dit vereist nog een vraag aan Arjen Gerritsen. Want hij is niet alleen lid van een VNG-commissie die GIBIT propageert, maar ook voorzitter van Gebruikersvereniging Centric. Heeft hij zijn leden niet van de GIBIT-zegeningen kunnen overtuigen? En wringt dat dragen van twee petten niet?

Gerritsen ziet geen andere pet. “Het moet twee kanten op werken. Absorptie bij leveranciers is minstens zo belangrijk als bij gemeenten. De VNG heeft een algemene taak. De gebruikersvereniging is specifiek gericht op Centric-gemeenten. Leden vragen zich af welke invloed GIBIT heeft op bestaande afspraken. De vereniging heeft een onafhankelijke positie tegenover de leverancier, maar niettemin is er wat opgebouwd. Past GIBIT in dat evenwicht?” Dat willen GV-leden en Centric dus uitgezocht zien. De voorzitter laat alvast weten: “Ik geloof van wel.”

Absorptie bij leveranciers is minstens zo belangrijk als bij gemeenten

stelling was om gemeenten bewust te maken van alle aspecten om een goed opdrachtgever te zijn. Anders zou je een ruim raamwerk krijgen en kon je het net zo goed niet doen.”

Over de risicoverdeling zegt hij: “De deskundigheid zit bij de leverancier. Die weet wat gemeenten nodig hebben. Dat heeft consequenties voor de risicoverdeling. GIBIT is niet onredelijk. Ik snap de kritiek, maar weet ook wie het zegt. We zijn er echt niet op uit om goedkoop in te kopen of marktpartijen te knevelen.”

Voor dat laatste ziet Gerritsen ook geen aanleiding. De vraag hoe na ‘Elias’ de verhouding tussen gemeenten en ICT-aanbie-

‘Waarom zo uit de pas lopen?’

Ruud Leether: “Je moet als overheid één juridische taal spreken”

Slecht leesbaar, juridisch rammelend. Dit zou noch de markt, noch de overheid moeten willen. De omschrijvingen die Ruud Leether voor de GIBIT geeft, zijn weinig flatteus. En als voormalig legal counsel bij het ministerie van VenJ weet hij waar hij over praat. Hij was voorzitter van de werkgroep die de ARBIT, de IT-inkoopvoorwaarden voor het rijk, heeft opgesteld. Leether constateert dat de definitieve versie van de GIBIT vol staat met onduidelijke formuleringen en juridische gebreken, maar dat is niet eens zijn grootste bezwaar.

“Ik had begrepen dat ze de ARBIT als basis zouden gebruiken. Mijn conclusie is dat dat nauwelijks is gebeurd. Ik vind dat uit de pas lopen maatschappelijk buitengewoon ongewenst. Je moet als overheid juist één juridische taal spreken naar de markt en dat kan ook heel goed.”

In de motivering voor de gemeentespecifieke inkoopvoorwaarden herkent Leether zich niet. “Flexibiliteit, aantoonbaar gebruik van standaarden, veiligheid en het aansluiten op cloudontwikkelingen – wat is daar nou gemeentespecifiek aan? Dezelfde problemen spelen natuurlijk ook bij de rijksoverheid. En dat de ARBIT niet flexibel genoeg zouden zijn voor het meenemen van licenties is onzin, net als dat ze te veel gericht zouden zijn op maatwerk.”

Formuleringen als ‘niet aanvaardbaar voor opdrachtgever’, ‘prijsstijgingen die niet voorzienbaar zijn’, ‘tekortkoming van niet ondergeschikte aard die ten nadele is van opdrachtgever’ – “wie kan daar nu iets mee?” Maar het gaat verder dan slordig opschrijven. “Er staan tal van bepalingen in die onmogelijke bewijslasten voor de leverancier met zich meebrengen. ‘Preventief en innovatief onderhoud moet ertoe bijdragen dat de ICT-prestatie tijdig zal voldoen.’ Wie bepaalt wat tijdig is?”

Daarnaast zijn er duidelijke verschillen met de ARBIT. “Belangrijke onderwerpen als aansprakelijkheid en intellectuele eigendomsrechten zijn anders geregeld en wat het laatste onderwerp betreft ook nog volstrekt onbegrijpelijk. Conversie, implementatie en onderhoud maken standaard onderdeel uit van de opdracht. In de ARBIT moet dat allemaal afzonderlijk worden gecontracteerd. Waarom zulke andere uitgangspunten?”

Leether is nog steeds lid van de ARBIT-werkgroep, die een paar keer per jaar bijeenkomt. Hij wil niet kinderachtig overkomen. “Ik ben de GIBIT niet gaan lezen in de hoop te kunnen concluderen dat de ARBIT beter zijn. Ik hoopte op wat moderniseringsslagen waar we met de werkgroep iets mee zouden kunnen.” Eigenlijk vindt hij alleen de risicoanalyseverplichting in artikel 3.5 een interessant idee om in de ARBIT-werkgroep te bediscussiëren. Gemeenten zullen volgens Leether onvoldoende kennis hebben om de GIBIT goed te kunnen beoordelen. “Daarom was het zo belangrijk daar in een eerdere fase met de ARBIT-werkgroep over in gesprek te gaan. De VNG was daarvoor ook al bij de start van ARBIT-werkgroep uitgenodigd. Dit zijn helaas gewoon geen goede voorwaarden.”

Leren luisteren

De televisie stond aan; journaal en kerstboom vlak naast elkaar. Een jong gezin woonachtig in Slotervaart, de nieuwbouwwijk van Amsterdam die na de oorlog de redding was voor het jonge gezin Van Hees. Het leven was overzichtelijk en het nieuws kwam via journalistiek de huiskamer binnen. Meestal via de TV; krantenlezen was er voor de kinderen niet bij. Herinneringen uit die tijd bestaan uit flarden van beelden van de landing van de Apollo op de maan en relletjes op de Dam. “Mama, wat is het rode boekje?” hoor ik mezelf nog vragen. Mijn moeder ontweek het antwoord; het weghouden van communistische idealen leek haar het beste. De angst voor de Russen zat er diep in en werd ons met de paplepel ingegoten. En die zat diep merkte ik toen in Berlijn de muur voel en ik huilend op de bank met mijn eerste kind op schoot naar de beelden op televisie keek.

Zet deze wereld af tegen de wereld waarin kinderen tegenwoordig opgroeien. Een overvloed aan informatie, geen bescherming tegen onwelgevallig nieuws. Vrijheid van meningsuiting als principe haalt de wereld binnen van gefundeerde en ongefundeerde meningen van Jan en alleman. Via social media en allerlei sites komen beelden van verschrikkelijke gebeurtenissen binnen op de smartphones die kinderen zelf in de hand hebben. Het achterhouden van informatie is achterhaald. We zijn verontwaardigd als in China bepaalde sites of social media geblokkeerd zijn. In het westen mogen we bijna alles zien en is het moeilijk te zien welk nieuws juist is en waarop je een mening moet baseren. Deskundige journalisten moeten mee in de hype en worden verdrongen door de impact van social media en de directe impact daarvan in het nieuws. Van een veilig opvoedingsklimaat is geen sprake meer.

Welke beoordeling moeten wij geven aan al deze ontwikkelingen? De politiek zoekende en de rechter komt eraan te pas; wie mag wat zeggen over wie? De zin en onzin die wordt verkondigd is de dag daarop niet weg als de vis in de krant is verpakt. Nee, alles wat je zegt kan al verspreiding krijgen; van gecreëerd nieuws is niet meer af te komen. Directe democratie krijgt een wind mee, maar zonder dat de voorstanders zich druk maken over de kwaliteit van de berichtgeving en de manier waarop mensen komen tot meningsvorming. De voor de hand liggende reflex bij alle nieuws is dat mensen eerst de emotie voelen en pas daarna gaan analyseren en nadenken over het waarom. Politici en journalistiek zijn schatplichtig te zorgen voor een veel betere informatievoorziening aan burgers over wat er te kiezen valt. En het aanleren van de houding bij kinderen dat je niet alles moet geloven wat je wordt gezegd of op internet te vinden is. Leren luisteren begint thuis aan tafel.

Marijke van Hees
Zelfstandig ondernemer en raadslid Enschede

Privacybewustzijn gevraagd

Privacybewustzijn begint bij de bestuurder, want het gaat om juridische interpretatie, goed ontwerp, ketensamenwerking, rapportage én beveiliging. Zoiets delegeer je dus niet simpelweg naar bijvoorbeeld een ICT-afdeling. En om de aanstelling van een goede Functionaris Gegevensbescherming kan die bestuurder niet meer heen.

Freek Blankena

Over krap anderhalf jaar is de Algemene Verordening Gegevensbescherming (AVG) van kracht en de Meldplicht Datalekken is er al een jaar. Privacy moet 'tussen de oren' bij al diegenen die met persoonsgegevens omgaan, of dat nu ICT'ers, inspecteurs, hulpverleners of beleidsmedewerkers zijn. En de nieuwe wetgeving maakt bestuurders daarvoor in hoge mate verantwoordelijk. Privacy is niet alleen een kwestie van goed beveiligen, maar ook van goede ketensamenwerking, het goed ontwerpen van processen en systemen (Privacy by Design) én het goed interpreteren van de wetgeving. Dat betekent veel huiswerk voor overheden.

Privacy is bij gemeenten zeker een punt van aandacht, zegt Martine Meijers, coördinator privacy bij de VNG. "Met name in het social domein is daar de afgelopen jaren in geïnvesteerd." Afgelopen voorjaar kwam volgens haar het besef dat de inspanning wel wat groter, structureler en strategischer mocht, mede door de komst van de AVG. "Er verandert wat door de AVG, en de vraag wat privacy eigenlijk ís in de informatiesamenleving komt steeds meer op."

Zij ziet de gemeenten enerzijds steeds meer in een regiepositie geplaatst, waarbij ze met persoonsgegevens werken die ze soms ook moeten delen. Anderzijds moeten ze het grondrecht privacy waarborgen. "Dat wordt steeds ingewikkelder en misschien hebben we daardoor een achterstand in denken en doen."

Ondertussen moet er natuurlijk wel gewoon aan wetgeving worden voldaan, in alle domeinen. Meijers: "Het is niet zo dat er geen dingen fout gaan in het sociaal domein, maar wat we daar aan het doen zijn – gemeenten en ketenpartners samen, soms met commentaar van de AP hoe het nog beter kan – die beweging moeten we op alle domeinen gaan maken."

Cyclus

Ad Reuijl is directeur van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP), een netwerkorganisatie die vanuit met name de ZBO's is ontstaan en die zich steeds meer richt op privacybescherming. Ook hij constateert dat er nog werk aan de winkel is. Reuijl neemt de eerdere invoering van de Baseline Informatiebeveiliging Rijk (BIR) als voorbeeld. Ook dat is een leerproces. "Er zijn in de praktijk verschillende manieren om die te volgen. Een manier die ik niet zo toejuich is het gebruik als afvinklijst. Je moet het eerder als een levend normenkader hanteren. Risicobewust en risicogestuurd omgaan met de vraag waar nu de risico's in je bedrijfsvoering zitten en waar je kroonjuwelen. Zodat je een cyclus in gang brengt, waarmee je je informatiebeveiliging jaarlijks verbetert. In de top van de cyclus zit de bestuurder die steeds weer geconfronteerd wordt met de risico's die nog niet gedekt zijn en waarover hij ook rapporteert."

De Privacy Baseline die CIP heeft ontwikkeld kan een zelfde rol vervullen, aldus Reuijl. "Datalekken zijn niet altijd te voorkomen, maar wat je wél kunt doen, is zorgvuldig zijn en je privacy governance op orde brengen. Dan kun je ook op meer coulance

Privacy moet je goed beschermen, zegt de wet, en de komende Europese regelgeving legt de lat nog wat hoger. Dat brengt een flinke verantwoordelijkheid met zich mee voor overheidsbestuurders. Niet eenvoudig, want privacy kent vele aspecten. In deze iBestuur-special 'Grip op privacy' – onder redactie van Marc van Lieshout (TNO), Ad Reuijl (CIP) en Theo Hooghiemstra (PBLQ) – behandelen we die aspecten. De artikelen gaan in op de bestuurdersverantwoordelijkheid, de maatschappelijke kanten, de juridische aspecten, beveiliging en 'privacy by design'.

iBestuur symposium

De iBestuur-special 'Grip op privacy' is de opmaat naar het gelijknamige iBestuur symposium op 7 februari 2017. De vele aspecten van privacy komen aan bod: maatschappelijk, juridisch, bestuurlijk, technisch en dat van de informatiebeveiliging. De casus van het ministerie van VenJ loopt als een rode draad door het programma. Met onder andere Siebe Riedstra *(SG minVenJ)*, prof. Jeroen van den Hoven *(TUDelft)*, Wilbert Tomesen *(Autoriteit Persoonsgegevens)*, Marens Engelhard *(Algemeen Rijksarchivaris)*, Marjolein ten Kroode *(Raad van Bestuur, GGZ Rivierduinen)*, Sandor de Coninck *(CISO Rijkswaterstaat)*, Steven Luitjens *(directeur Informatiesamenleving en Overheid, minBZK)*, José Lazeroms *(Raad van Bestuur, UWV)*.

Meer informatie op ibestuur.nl

Grip op privacy is een samenwerking van iBestuur met PBLQ, SIG, SYSQA, TNO, CIP-overheid en KPN.

rekenen van de Autoriteit Persoonsgegevens in het geval dat het toch een keer fout gaat. De Privacy Baseline is hierbij een hulpmiddel. Die stelt je in staat een proces te verankeren in de organisatie, waarmee de bestuurder daadwerkelijk verantwoordelijkheid neemt voor wat er gebeurt en kan sturen op risico’s.”

Net als Meijers ziet Reuijl het spanningsveld waarin overheidsorganisaties opereren. Afscherming van persoonsinformatie tegen ‘de buitenwereld’ is één ding, bescherming van die informatie tegen ‘de overheid’ zelf is iets anders. Reuijl: “Met het oog op opsporing en voorkoming van criminaliteit, aanslagen, et cetera zou je soms meer willen gebruiken dan nu mag. Veel is mogelijk, maar niet alles is wettelijk toegestaan. De wet loopt soms gewoon achter.”

Toelaatbaarheid

Binnen het CIP-netwerk kwam onlangs een discussie voorbij over de vraag of het gerechtvaardigd is om het inkomen van ouders na te gaan van jongeren die bijstand aanvragen. “Dan moet je de Suwi-wet erbij pakken en je afvragen waar die informatie zit en of het gebruik nog voldoet aan de doelbinding van die registratie. Daarnaast wordt het begrip ‘gerechtvaardigd belang’ steeds belangrijker. Mij valt op dat in heel veel situaties interpretatie nodig is.”

Juist dat soort afwegingen pleit voor de aanstelling van een Functionaris Gegevensbescherming, een soort ‘gewetensfunctie’ binnen de organisatie. Reuijl: “Maar er zijn grote organisaties die dat nog niet hebben gedaan en dat is jammer. Als bestuurder laat je zien dat je die privacy-agenda en het toezicht heel duidelijk belegt. Dit is overigens een van de verplichtingen die meekomen in de AVG. Ik raad iedereen aan om hierop al vooruit te lopen.” Uit een CIP-enquête van eind 2015 bleek 35 procent van de overheidsorganisaties een apart benoemde FG te hebben en bij ongeveer de helft van de organisaties was privacy belegd als specifieke verantwoordelijkheid bij een van de bestuursleden. “Bij het UWV bijvoorbeeld is privacy belegd bij de voorzitter. Het is daarmee gescheiden van de ICT-verantwoordelijkheid, die ligt bij een bestuurslid.”

Ook Meijers noemt de AVG-verplichting tot het aanstellen van een Functionaris Gegevensbescherming een belangrijk punt. Ze heeft op enkele netwerkbijeenkomsten daarover gemerkt dat die functie door zeer uiteenlopende mensen wordt ingevuld, zowel mensen met een technische achtergrond als met een meer juridische achtergrond. Hoe die functie exact moet worden ingevuld is nog onderwerp van Europees overleg, maar er moet in ieder geval niet licht over worden gedacht.

Aan Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens, de vraag of iemand die FG-functie ‘erbij kan doen’ of niet. “Alles draait om de onafhankelijkheid en deskundigheid van de FG”, zegt hij. “Onafhankelijkheid is als eis in de AVG vastgelegd, maar moet ook de persoon typeren. Want dán is de FG uiteindelijk het meest van waarde voor de organisatie. Natuurlijk mag er geen belangenverstrengeling zijn. Dit betekent dat de FG binnen de organisatie geen andere functie mag hebben waarin hij, zoals dat heet, ‘het doel en middelen van een gegevensverwerking bepaalt’.” Bij een managementfunctie, zoals hoofd ICT, is volgens Tomesen die belangenverstrengeling bijvoorbeeld al snel aan de orde. “De organisatie moet daar scherp op zijn.”

Daarnaast is voor de functie van FG specialistische kennis nodig. “Organisaties moeten kijken wat er in hun specifieke geval nodig is; het concrete kennisniveau dat noodzakelijk is, ligt bijvoorbeeld hoger als een organisatie grote hoeveelheden gevoelige gegevens verwerkt. Op basis van zulke afwegingen – over belangenverstrengeling, de aard van de gegevens die worden verwerkt en de vereiste vakkennis – kan een organisatie besluiten de taken van de FG bij een bestaande werknemer te beleggen óf om hiervoor speciaal iemand in dienst te nemen dan wel in te huren. Een onafhankelijke FG, die heel goed weet waar hij het over heeft, is het beste in staat het privacybewustzijn in zijn organisatie, van hoog tot laag, te bevorderen.”

Fundamenteel

Privacybewustzijn moet zich binnen organisaties dus los van de dagelijkse beslommeringen ontwikkelen. Ondertussen moeten de regels wel nageleefd. Reuijl ziet nog een wat afwachtende houding ten opzichte van de AVG. “Maar begin daar nou mee. Een aantal grote organisaties doet al analyses. Je kunt via CIP ook te rade gaan bij collega-organisaties. En inderdaad: benoem een privacy officer, een FG. En dat is dan dus níet het hoofd IT-beveiliging. En gebruik de Privacy Baseline die we hebben ontwikkeld en voer Privacy by Design in, in je ontwikkelafdelingen. Dan adresseer je meteen veel punten van die AVG. Als de manager hanteerbare instrumenten in handen heeft dan helpt dat. En misschien nog belangrijker: als je privacybescherming op orde hebt, dan bouw je aan het broodnodige positieve imago van de overheidsdienstverlening.”

Meijers: “Wij hanteren twee sporen. Het eerste is dat de basis op orde moet, maar het tweede spoor is dat we echt het gesprek moeten gaan voeren, fundamenteel, als overheden met elkaar en met de maatschappij: wat is privacy nu in deze informatiesamenleving? Welke waarden proberen we daarmee te beschermen? Zijn onze huidige wetten en concepten nog bruikbaar? Mensen verwachten een proactieve regievoerende overheid en tegelijkertijd zijn er grenzen aan wat je met gegevens kan doen, dus daar moet je het over hebben. Ondertussen moeten we zorgen dat we ons binnen het huidige juridische kader begeven. Daar moet de burger op kunnen vertrouwen.”

Open Data bevordert transparantie en stimuleert marktpartijen tot innovatie. Maar in het combineren van open data met andere informatiebronnen schuilen ook bedreigingen voor de privacy.

‘Burger heeft recht op zorgvuldige overheid’

‘Open Data, tenzij’. Dat is de verplichting die de Nederlandse overheid zichzelf heeft opgelegd in de Nationale Open Data Agenda 2016. ‘Overheidsdata stimuleren marktpartijen tot innovatie, nieuwe businesskansen en werkgelegenheid. Inzicht in de beschikbare data en informatie van de overheid kan bijdragen aan kostenreductie en aan verbetering van beleidsprocessen’, aldus minister Plasterk in een Kamerbrief van november 2015.

Er zit schot in. Internationaal scoort Nederland hoog in het beschikbaar stellen van datasets. Maar er zijn ook verschillen tussen ministeries en zeker ook tussen landelijke en lagere overheden. Gemeenten zijn gemiddeld minder ver. Dat is niet per se onwil, stelt onderzoeker Victor Klos van TNO: “Ze hebben soms zelfs geen volledig inzicht in welke datasets ze hebben. Daarbij komt dat gemeenten er de laatste jaren tal van verantwoordelijkheden hebben bij gekregen.”

Terughoudendheid komt ook voort vanuit zorg om de bescherming van persoonsgegevens. Jean-Louis Roso van TNO: “Het ministerie van IenM was een voorloper rond het gebruik van open data. Niet helemaal toevallig. Zolang het om niet-persoongebonden data gaat zoals vervoersstromen en dergelijke, is er geen probleem. Maar bij veel andere datasets, zeker op het gebied van volksgezondheid, is er kennis nodig om te bepalen welke data je veilig kunt aanbieden en op welk aggregatieniveau. Simpelweg anonimiseren door de kolom NAAM te verwijderen is bijvoorbeeld vaak niet voldoende. We zien dat veel overheidsorganisaties worstelen met privacy-vraagstukken. Daarom hebben we vanuit verschillende onderzoekstrajecten een management- en beheermodel ontwikkeld voor open data: BOMOD. Daarin worden de stappen beschreven die je moet doorlopen om datasets verantwoord ter beschikking te stellen.”

Verantwoordelijk

Naar de letter van de nieuwe Europese privacyverordening (AVG) blijft de dataleverende partij verantwoordelijk voor beschikbaar gestelde data. Als een derde partij onzorgvuldig met die gegevens omspringt, kan de oorspronkelijke datahouder daar dus op worden aangesproken.

Volgens Klos ligt in anonimiseren lang niet altijd de oplossing. “Wat er gebeurt is dat open data door bedrijven worden gecombineerd met grote hoeveelheden gesloten data. Door combineren en analyseren blijkt vervolgens toch veel informatie te kunnen worden teruggevoerd naar specifieke groepen of zelfs individuen.” Dat dreigt bijvoorbeeld bij medische gegevens, waarvan gezondheids- en fitness-apps op smartphones er steeds meer opslaan.

Zodra het over burgers en gedrag van burgers gaat, is het lastig om te bepalen tot op welk detailniveau datasets kunnen worden aangeboden. Roso raadt daarom grote organisaties, zoals ministeries, aan naast een ‘security officer’ ook een ‘privacy officer’ aan te stellen. “De overheid moet heel goed gaan nadenken over ‘privacy by design’. Privacy moet niet los worden gezien van andere datavraagstukken.”

Versleuteling

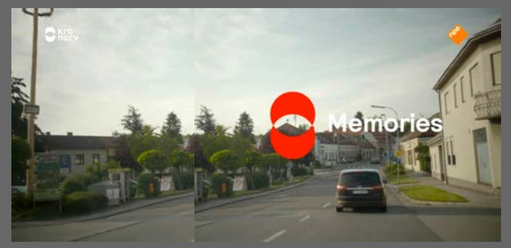
Om de potentie van open data toch te kunnen waarmaken is volgens Klos een paradigma-verschuiving nodig. “De burger heeft recht op een zorgvuldige overheid. Dat is de kern van de democratie. Waar wij naar zoeken is een manier om wel de belofte van geavanceerde data-analyse en van nieuwe toepassingen in stand te houden, zonder dat persoonlijke gegevens op straat kunnen komen. De idee van Big Data is dat je veel datasets in een grote bak gooit en daarmee je ‘magic’ doet. Daar worden indrukwekkende resultaten mee geboekt, maar in veel gevallen zal de aanpak niet voldoen aan de nieuwe Europese richtlijn. De toekomst zit volgens ons onder andere in encryptie.”

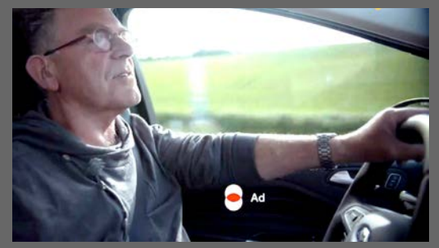
TNO zoekt het in een nieuwe vorm van versleuteling: homomorfe encryptie. Er loopt nu een proefproject in de medische sector waar deze technologie wordt beproefd. In deze proef – PRANA-DATA – gaan diverse partijen en personen gezondheidsgegevens uitwisselen zonder het risico dat persoonlijke data worden uitgewisseld (zie kader). Met homomorfe encryptie is het mogelijk om een dataset op zodanige wijze te versleutelen dat andere partijen er vragen aan kunnen stellen, zonder dat ze ooit de bronbestanden te zien krijgen. De wijze van versleuteling bepaalt welke vragen mogelijk zijn. Vooral in een medische setting, waar veel partijen en individuen eigenaar zijn van datasets, zou deze route mogelijkheden bieden om gedetailleerde persoonsinformatie te benutten, zonder dat de privacy in het geding komt.

Deel analyse, geen data

In het onderzoeksproject PRANA-DATA wordt een case uitgewerkt waarbij partijen en personen medische gegevens uitwisselen zonder risico op het weglekken van persoonlijke data. Privacy-problemen ontstaan doordat toepassingen gevoelige gegevens nodig hebben om zinnige analyses te maken. Ook geanonimiseerde gegevens blijken in combinatie met andere datasets vaak tot personen terug te leiden. TNO beproeft in PRANA-DATA een technologie waarbij derde partijen alleen met vercijferde data werken. In het project PRANA-DATA wordt de praktische toepasbaarheid van deze veelbelovende technologie onderzocht. Zodra je kunt rekenen met versleutelde data, opent zich een wereld van toepassingen, zonder dat de privacy van individuen in gevaar komt.

Meer hierover op www.pranadata.nl.



'Memories', 'Ik vertrek' en medische tv-programma's: privacy wordt ondergeschikt aan de zucht naar aandacht.

De barricades op voor onze privacy!

Leidt datagraaien tot datacrisis of keert de wal het schip?

Moeten we gewoon accepteren dat privacy nu eenmaal minder belangrijk wordt in het Facebook-tijdperk en nu de roep om veiligheid steeds luider klinkt? Of is het data-armageddon nabij met Big Brothers als Poetin, Xi en Trump aan de macht? We moeten niet passief blijven, vindt hoogleraar Jeroen van den Hoven. Bedrijven en burgers moeten opstaan voor databescherming.

Peter Olsthoorn

Wie heeft er geen geheimen voor z'n partner? Tachtig procent steekt z'n hand op. Wie wil er dus al z'n berichten en zoekopdrachten delen met de partner? Handen in de zaal blijven nu omlaag. Nog zo eentje: ik was altijd tegen de opslag van metadata van het bellen en mailen door justitie. Tot ik het slachtoffer werd van straatgeweld en de politie de agressor vlot traceerde dankzij diens telefoondata.

Nog een: Brigitte van Blijswijk van ABN Amro heeft autisme, Klaas Pieter Derks (37) van UWV lijdt aan depressies. Het stond in een NRC-artikel, waarin redacteur Monique van Oostrum haar bipolaire stoornis openbaarde. Zo'n 3 miljoen mensen met psychische klachten telt Nederland, van wie 700.000 gediagnosticeerde geesteszieken. De meesten willen dat niet langer verhullen. Maar de werkgever dan?

Wat te denken van het opgeven van privacy om aandacht en mededogen te winnen? 'Memories' met Anita Witzier, 'Ik vertrek' en medische tv-programma's; privacy vloeit over de toonbank in de zucht naar aandacht. Om nog niet te spreken van een onophoudelijke stroom van ontboezemingen op Facebook.

De rem is eraf, waarom zeuren over privacy? Aan de andere kant: grote concerns kunnen ons griezelig nauwkeurig profileren en slechten privacygrenzen. En Rusland, China en ook Engeland voerden recent strenge wetgeving voor opsporing in, met privacy als verliezer. Trump kondigde iets soortgelijks aan. Uitpuilende datareservoirs staan hen ter beschikking.

En beschermen we onze vrije samenleving door de AIVD meer wettelijke bevoegdheden te geven, of bieden we mogelijke toekomstige dictators dan juist de poort naar totale controle? Wie het weet, mag het zeggen.

'Cryptocalypse'

Datadoemscenario's winnen terrein. Peter Schwabe van de Radboud Universiteit voorspelt de 'cryptocalypse', een einde aan dataveiligheid. Gedragsvoorspelling met big data rukt mondiaal op, met programma's als Beware van Intrado dat uit onze handelingen en uitingen de kans op wetsovertreding bepaalt. Onze eigen Belastingdienst maakt van iedereen een profiel dat je zelf niet mag inzien.

Het verst ging de waarschuwing dat oorlog en datadictatuur ons voorland zijn, met 'Feodalisme 2.0', 'Fascisme 2.0' en/of 'Communisme 2.0'. Ontwrichting dreigt, zoals die bij alle historische overgangen naar nieuwe samenlevingen optrad, nu door ongebreideld IT-gebruik. Deze theorie huldigt Dirk Helbing, in Zürich hoogleraar IT-sociologie en aan de TU Delft leider van het programma 'Engineering Social Technologies for a Responsible Digital Future'. Hij is mede door bemiddeling van Jeroen van den Hoven, hoogleraar ethiek en oud-decaan van de faculteit Techniek, Bestuur en Management, naar Delft gekomen.

Wat moeten we met zijn datahel en -verdoemenis? Zwaar overdreven, net als de schouwburgen vol jongeren met privacyzorgen die De Correspondent vult? Van den Hoven: "Nee, Helbing is als een idioot bezig om iedereen wakker te schudden en terecht. We begonnen het debat te laat en gaven belangen uit handen door de neoliberale overschatting van de markt, als het gaat om het behartigen van het publieke belang. Bedrijven mochten vrijelijk datagraaien en ons profileren uit naam van economische groei. Dat is lastig terug te draaien."

Wal keert schip

Dus staan we, aldus Helbing, op een kruispunt: gaan we naar centralistisch geleide – 'feodale' – staten die samen met concerns dankzij data en kunstmatige intelligentie de samenleving top-down sturen en volkeren controleren en exploiteren? Of kiezen we voor democratischer, bottom-up samenwerking waarin burgers zeggenschap over data verwerven, voor toepassingen die primair zijn gericht op ondersteuning?

"Het dreigt al verkeerd te gaan nu Trump de investeerder in databedrijven Peter Thiel en grondlegger van databroker Palantir de baas maakt over Amerika's informatie- en databeleid", vult Van den Hoven in. Toch betoont hij zich optimistischer dan Helbing over ontsnappingsroutes: "Ik benadruk liever het positieve, steek graag mensen een hart onder de riem en wil het bedrijfsleven meekrijgen. Deze datacrisis biedt ook kansen. Net zoals de ondernemingen die toekomstkeuzes maken met schone energie straks een betere positie hebben dan de bedrijven die dit nalaten."

Dus de markt kan het dataprobleem oplossen? "Nee, de mogelijkheden voor win-win zijn talrijk, maar je moet bijsturen. Olieconcerns gingen pas nadenken over windenergie onder dwang van internationale verdragen, nationale wetten en publieke opinie."

Van den Hoven schetst verregaande verwantschap tussen klimaatverandering en nieuwe houdingen tegenover datagebruik: weg met de naïviteit, en inhaalacties gaan bedenken. De

Zeven vragen

	Gerrit-Jan Zwenne, Universiteit Leiden en Brinkhof Advocaten	Daphne van der Kroft Bits of Freedom	Diana Janssen, directeur van marketingbrancheorganisatie DDMA
1. Welke partijen bedreigen de privacy van burgers momenteel het meest en waarom?	Onmiskenbaar de overheid. Zoals gemeenten voor doelmatige bemoeizorg, inlichtingendiensten met sleepnetten, hackende rechercheurs, Lodewijk Asscher die SyRI mogelijk maakt, Stef Blok die een Rotterdam-wet 2.0 bedenkt.	Zowel overheid als bedrijfsleven op grote schaal. Bij de overheid de Belastingdienst met koppeling van heel veel bestanden; in het bedrijfsleven Google en Facebook en de grote datahandelaren die in de schaduw opereren zoals Acxiom of Experian.	Vooral partijen waarvan je niet weet wat ze verzamelen, voor welke doeleinden en zonder dat ze transparant hoeven zijn. In de eerste plaats de veiligheidsdiensten. Maar ook overheden die bestanden koppelen zonder dat we weten wie daar toegang toe hebben en voor welke doeleinden.
2. Is vergaren van data ook een privacyschending en waarom wel/niet?	Het verzamelen van persoonsgegevens kan al een 'chilling effect' hebben, ook als er (nog) niks mee wordt gedaan. Een videocamera maakt al inbreuk, we weten niet wanneer die aanstaat, wie de beelden bekijken en welke conclusies zij trekken.	Te vaak weten we niet hoe we geprofileerd worden. Privacy gaat over autonomie, eigen controle en keuzes. Wij kunnen te vaak geen controle uitoefenen op de gegevensverzameling en het gebruik ervan.	Als je je aan de wet houdt is data verzamelen geen privacyschending. Er zijn duidelijke regels wat mag en wat niet. Maar er is meer nodig dan lijstjes afvinken. Partijen moeten uitgesprokener en transparanter worden over hun visie op data, over hun motivatie en intenties om data te verzamelen en te gebruiken.
3. Welke adviezen kun je geven aan mensen die wel bang zijn?	Geen aluminiumfolie hoedjes. Geen privacy paranoia. Wel incognito browsen. Adblockers gebruiken en VPN-providers die je een random IP-adres bieden. Enz.	Je zorgen zijn terecht. Digitale technologie heeft ons zoveel gebracht maar noodzakelijk vertrouwen staat op het spel. Gebruik onze Internetvrijheid Toolbox en oefen druk uit op overheid en politiek.	Angst komt vaak voort uit gebrek aan informatie. Je kunt grofweg drie typen mensen onderscheiden: Pragmatici, Sceptici en Onbezorgden. Mensen die bang zijn, geven relatief vaak aan dat ze niet begrijpen hoe de online wereld werkt.
4. Wat zeg je mensen die beseffen dat ze wat te verbergen hebben, maar zich geen privacyzorgen maken?	Fijn voor je! Weet je het zeker?	Je ziet de ijsberg niet, hoe er profielen worden opgebouwd met kansberekening hoe je bent en reageert en wat jij krijgt voorgeschoteld; bijvoorbeeld de ticketprijs of straks de zorgpremie. Een steeds groter deel komt boven water, let maar goed op!	Gefeliciteerd. Dan heb je het blijkbaar goed op orde. Ik ben zelf een pragmaticus. Ik maak een afweging wat ik wil delen. Ik merk dat ik het imago van organisaties steeds belangrijker vind bij die keuze: hoe staat een bedrijf in de data discussie? Hoe open zijn ze over waarom ze mijn data vragen en wat ze daarmee doen?
5. Wat zeg je tegen mensen die bewust privacy opgeven omdat ze er sociaal heel veel voor terug krijgen?	Het ene hoeft het andere niet uit te sluiten.	Je geeft steeds meer op en maakt je afhankelijk van grote spelers en transparant voor overheden die je in hokjes stoppen.	Je geeft privacy op in ruil voor sociale diensten. Dit gebeurt bij elke sociale interactie, maar met digitale data gebeurt dit op een andere schaal. Wees je daar bewust van.
6. Is de privacyverordening van 2018 goed (genoeg) en waarom wel en niet?	Neen. Maar iets beters is misschien ook nog niet haalbaar. We hebben geen idee hoe privacy te beschermen met wet- en regelgeving.	Gezien de enorme lobby van bedrijven zijn we positief verrast. We hopen op hoge boetes als stok achter de deur zodat bedrijven zich aan de regels gaan houden. Zorgen blijven, over profilering en automatische beslissingen vanuit data.	Het is een pluspunt dat alle partijen die zich richten op de Europese markt zich in elk land aan dezelfde regels moeten houden. De verordening is technologieneutraal, op principes gebaseerd en gericht op meer transparantie. Maar hij blijft helaas complex.
7. Gebruik je zelf Facebook, Google, Gmail, Whatsapp, Instagram, Amazon, Bol.com et cetera?	Google, Gmail, Whatsapp, Bol.com: ja; de rest neen, maar niet om principiële redenen.	Bits of Freedom bereikt via Facebook belangrijk publiek. Google en Gmail zelf ook, Amazon, Bol.com. Whatsapp is onmisbaar voor werk en privé, maar onder collega's gebruiken we Signal.	Ja, ik gebruik veel, maar niet alles heel vaak. Ik wil weten hoe de verschillende platforms en apps werken. Wat bieden ze, hoe gebruiksvriendelijk zijn ze? En – beroepsdeformatie – word ik goed geïnformeerd over data?

nieuwe EU-privacyverordening van 2018 volstaat niet. "Nu al treft de Europese Commissie strengere mededingings- en privacymaatregelen tegenover de grote spelers."

Europa staat daarin echter vrij geïsoleerd ten opzichte van China, Rusland en straks de VS, waar overheden en bedrijven elkaar vinden in het 'datagraaien'. Van den Hoven: "Overheden en ondernemingen die kiezen voor hoge morele standaarden, hebben het momenteel lastig. Toch keert de wal het schip. Als het vertrouwen in overheden en in elkaar zo afneemt, legt dat de bijl aan de wortel van de samenleving die het van vertrouwen moet hebben en niet van controle."

Vrije markt

De oorlog en opstand van Helbing of het vredig herstel van Van den Hoven? De laatste: "Helbing hoopt ook op gezond verstand. Zo benadrukt Dirk dat privacy een cruciale conditie voor innovatie en creativiteit vormt. Samenlevingen met weinig respect voor mensenrechten, sociale verhoudingen, transparantie en privacy doen het slechter. Scandinavische landen, Duitsland en Nederland voeren de lijstjes van kwalitatief hoogstaande samenlevingen aan."

Maar ook wij kiezen voor meer controle voor veiligheid en kopen gratis diensten met bergen data. De voordelen wegen zwaarder. Van den Hoven: "Dus denk ik dat het keerpunt komt wanneer de exploitatie mensen in hun portemonnee gaat raken. Mensen pikken niet dat ze meer gaan betalen voor het vliegticket dan de buurman, op grond van wat aanbieders weten van je bereidheid om te betalen."

Dit betekent in feite ook het einde van de vrije markt, toont Van den Hoven slim aan, wat niemand wil: "Bij een volstrekt individuele relatie tussen aanbieder en klant op grond van de data met flexibele prijzen per individu is er geen markt meer."

Hij schetst in een uitstekend recent betoog nog meer concrete nadelen van datamisbruik en privacyschending: "Ik gooi de vaagheden zoveel mogelijk overboord. Behalve met economische exploitatie voelen mensen ook met sociale discriminatie en psychologische manipulatie straks keihard de nadelen van datamisbruik." Dus het principieel verdedigen van privacy heeft afgedaan? Van den Hoven: "Dat niet, maar direct voelbare nadelen voorhouden werkt beter dan diepgaande filosofische discussie. Natuurlijk moet je mensen ook waarschuwen dat ze straks extern gedetermineerd worden en zich niet meer vrijelijk zelf kunnen presenteren met hun eigen identiteit. Dat anderen dat doen op grond van data. Dat is een wezenlijk aspect van privacy, maar helaas op dit moment nu minder voelbaar te maken..."

Welke informatie heb je echt nodig?

Privacy is een bestuurlijke kwestie geworden en bestuurlijke vragen hebben meerdere invalshoeken. Daarom pleit PBLQ voor een meervoudig perspectief op privacy. Niet alleen juridisch, of alleen informatiekundig. En altijd strategisch-bestuurlijk.

De Meldplicht Datalekken en de Algemene Verordening Gegevensbescherming maken bestuurders – nog meer dan voorheen – verantwoordelijk voor het juist toepassen van privacywet- en regelgeving. Dat is ook nodig, want privacy staat dagelijks digitaal onder druk. Realistisch ogende phishing mails hengelen naar bank- en creditcardgegevens. Criminele organisaties azen op persoonsgegevens die zij kunnen doorverkopen op de zwarte markt of gebruiken voor identiteitsfraude. Ransomware bevriest bestanden die pas worden vrijgegeven na betaling van losgeld. Zowel zakelijk als privé komen mensen steeds vaker in aanraking met verschillende vormen van cyberdreiging. Ook neemt de berichtgeving toe over persoonsgegevens die op straat belanden. De reputatieschade voor de gehackte organisaties is groot. De noodzaak van het goed beschermen van persoonsgegevens van klanten en burgers staat hoog op de agenda van bedrijfsleven en overheid, weet Theo Hooghiemstra van de advies- en opleidingsorganisatie PBLQ. “Het bewustzijn dat men ‘iets’ moet doen is alom aanwezig en het gevoel van urgentie ook. De vraag die wij krijgen van opdrachtgevers is: wát moeten wij dan doen?”

Privacy als norm

Hooghiemstra en zijn collega Dirk Schravenveld pleiten voor een brede blik op privacy. Niet alleen juridisch of alleen informatiekundig, maar minimaal een combinatie van beide en dan ook steeds vanuit een strategisch-bestuurlijk perspectief. Tegelijkertijd moet rekening worden gehouden met de context van de gegevensverwerking, zoals bijvoorbeeld in de zorg of het onderwijs. “Privacy is een bestuurlijke kwestie geworden en bestuurlijke vragen hebben meerdere invalshoeken.” Dat lijkt misschien heel ingewikkeld, maar wanneer men digitale dienstverlening biedt moet privacy standaard onderdeel zijn van de discussies over functionaliteit. Het is geen apart onderwerp dat bij de juridische collega’s hoort of bij de informatiekundige. Privacy gaat iedereen aan en moet de normaalste zaak van de wereld worden.

Rekeningrijden

Waar te beginnen in de eigen organisatie? Schravendeel: “Vraag jezelf af wat daadwerkelijk nodig is aan persoonsgegevens om het werk te kunnen doen. De neiging is om te veel te vragen van de burger wanneer dit niet nodig is.” Hooghiemstra noemt als voorbeeld het rekeningrijden dat rond de eeuwwisseling hoog op de agenda stond en inmiddels weer terug is als punt van aandacht. “Toen die discussie voor het eerst werd gevoerd, werd er gesproken over camera’s op alle wegen om auto’s te kunnen volgen. Tot iemand vroeg of het wel nodig was om te zien waar iemand zich precies bevindt. Waarom geen kleurcode gebruiken voor de verschillende wegen? Of het nu de A12 is of de A4 maakt niet uit, gebruik rood, blauw en geel voor de verschillende toltarieven. Iedereen dacht aanvankelijk dat het noodzakelijk was om te weten waar mensen reden om het aantal kilometers in rekening te kunnen brengen. Nee, alleen de hoeveelheid kilometers en het soort weg telden.”

Hooghiemstra geeft nog twee voorbeelden. “Toen ik nog voor het College Bescherming Persoonsgegevens (de huidige Autoriteit Persoonsgegevens) werkte liet een gemeente burgers 106 vragen beantwoorden bij het aanvragen van huursubsidies. Als toezichthouder vroegen we welke persoonsgegevens echt noodzakelijk waren, gelet op het doel. Zes vragen bleken voldoende. Geen 106, maar zes. Het wetenschappelijke Nederlandse Huisartsen Genootschap (NHG) heeft zich gebogen over de vraag welke informatie noodzakelijk is voor tijdelijke waarneming in avonden en weekenden. Men hoeft niet alles van iemand te weten om die tijdelijke waarneming goed te kunnen uitvoeren, een professionele samenvatting is voldoende.” Dit zijn voorbeelden uit de ‘echte’ wereld, maar in de digitale wereld is vaak nog minder data nodig. Schravendeel: “Wanneer een jongere een fles wijn koopt moet hij een identiteitsbewijs overleggen. Daar staat op hoe hij heet, hoe lang hij is en wat zijn geboortedatum is. Het enige dat de wijnhandelaar moet weten: is deze persoon ouder of jonger dan 18? In de digitale wereld kunnen we een attributendienst aan de authenticatievoorziening toevoegen die alleen dát aan de webshop doorgeeft: rood is ‘te jong’, groen is ‘oud genoeg’. “

Noodzakelijk multidisciplinair

Hooghiemstra stelt dat de Algemene Verordening Gegevensbescherming (AVG) vergt dat bestuurders transparant zijn over en aansprakelijk voor de gegevens die zij verwerken:. “Burgers willen weten wat er met hun gegevens gebeurt en hebben daar ook het recht toe. Het juridisch perspectief en het informatiekundig perspectief kunnen en moeten worden gecombineerd. Multidisciplinaire teams zijn geen luxe meer, ze zijn noodzakelijk.” Schravendeel voegt daaraan toe dat PBLQ de benadering van het meervoudige perspectief toepast in workshops die zij geven met het Centrum voor Informatiebeveiliging en Privacybescherming (CIP). “Mensen uit verschillende organisaties en disciplines gaan een middag met een concrete casus aan de slag. Juist de onderlinge uitwisseling en het samen zoeken naar privacyvriendelijke oplossingen blijken heel vruchtbaar en worden door de deelnemers zeer gewaardeerd. Dezelfde benadering past PBLQ toe in een opleiding om privacy impact analyses (PIA) te leren uitvoeren. Die opleiding komt begin volgend jaar op de markt. Zo kunnen organisaties binnen de overheid voldoen aan de regelgeving, maar gaan ze ook zorgvuldig met de gegevens van de burgers om.”

U verkoopt wijn. Wat moet u van uw klant weten?

- [ ] Voornaam
- [ ] Achternaam
- [ ] Geboortedatum
- [x] Leeftijd
- [ ] Lengte
- [ ] Adres
- [ ] Postcode
- [ ] Woonplaats
- [ ] Geboorteplaats
- [ ] Geboorteland
- [ ] BSN
- [ ] Telefoonnummer (mobiel)
- [ ] Telefoonnumer (vast)
- [ ] Rekeningnummer (1)
- [ ] Rekeningnummer (2)
- [ ] BIC
- [ ] BTW-nummer
- [ ] KvK-nummer
- [ ] Kadastraal nummer
- [ ] Inlognaam
- [ ] Naam moeder
- [ ] Naam vader
- [ ] Locatie voertuig (start)
- [ ] Locatie voertuig (eind)
- [ ] Totaal kilometers
- [ ] Kenteken
- [ ] Merk auto
- [ ] CBR-registratie
- [ ] Haarkleur
- [ ] Verklaring goed gedrag
- [ ] etc.

Zes vragen bleken voldoende. Geen 106, maar zes.

… maar nog geen grip op beveiliging

Wie persoonsgegevens verwerkt moet ze goed beveiligen, zegt de wet. Maar bijvoorbeeld bij gemeenten maken de afhankelijkheid van leveranciers en het werken in ketens en over verschillende wetsdomeinen van de beveiliging een taaie klus.

Brenno de Winter

In de Wet bescherming persoonsgegevens (Wbp) staat het zo simpel: wie persoonsgegevens verwerkt moet ervoor zorgdragen dat dit veilig genoeg gebeurt. De data moeten volgens de wetgever beschermd zijn tegen verlies, enige vorm van onrechtmatige verwerking en onnodige verzameling. De plicht tot beveiligen legt duidelijk neer wat het doel van beveiliging is.

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. – Artikel 13 Wbp

Koudwatervrees

Voor het artikel spreken we negen 'chief information security officers' (CISO's), die geen van allen met naam of organisatie genoemd willen worden. Het onderwerp ligt politiek gevoelig en de angst om publiekelijk in problemen te komen is groot. Meerdere CISO's geven aan moeite te hebben met het goed in kaart krijgen welke risico's nu worden gelopen. Daarbij is er ook onzekerheid of alle geconstateerde risico's daadwerkelijk goed afgedekt zijn. In veel gevallen betwijfelen ze dat en is de vrees dat bij een incident niet aan de verwachting van het bestuur kan worden voldaan.

De Informatiebeveiligingsdienst (IBD), in 2012 opgericht door alle Nederlandse gemeenten, ondersteunt gemeenten in brede zin bij hun informatiebeveiliging en incidenten op dat vlak. Zij herkennen de vrees bij CISO's om open over beveiliging te praten. "Als je beveiliging heel goed doet vertel je er als je slim bent niet te veel over en als je het op punten niet op orde hebt ook niet", vertelt Nausikaä Efstratiades, hoofd van de IBD. "Voor veel mensen is het lastige materie of mensen denken dat het erg technisch is. Desalniettemin constateert de IBD dat gemeenten vooral open en transparant willen zijn over de wijze waarop zij met gegevens omgaan. Zij erkennen hun verantwoordelijkheid."

Ketenverantwoordelijkheid

Efstratiades wijst erop dat er bij gemeenten veel specifieke uitdagingen zijn, omdat er veel samenwerkingsketens zijn. "Denk alleen al aan bijvoorbeeld de jeugdketen, waarin gemeenten allerhande informatie uitwisselen met GGD, bureau Halt, Jeugdzorg, het OM en ga zo maar door", illustreert zij. "Dan is het niet voldoende om je eigen beveiliging op orde te hebben maar moet dat ook in samenhang met de ketenpartners worden geregeld." Het is in samenwerkingsverbanden niet altijd op het eerste gezicht en voor het gehele proces duidelijk wie welke rol heeft: is de gemeente bewerker of verantwoordelijke?

Voor beveiliging maakt dat laatste punt veel uit. De gegevensbewerker die verantwoordelijke is, blijft dat ook als een andere partij de gegevens verder bewerkt of een ICT-dienstverlener wordt ingeschakeld. Die verantwoordelijkheid wordt sinds

de invoering van de nieuwe wetgeving begin 2016 opeens in volle hevigheid gevoeld. Met alle worstelingen om zelf aan de verplichtingen te voldoen, is het goed toezicht uitoefenen op leveranciers voor de meeste security officers nog niet mogelijk.

Baselines

Als de problematiek wordt opgepakt dan wordt vaak aan leveranciers gevraagd om aan normen te voldoen. Populair zijn dan de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Gemeenten (BIG) of de ISO-27001/27002-normen. Maar het gebeurt ook wel dat de leverancier de leiding neemt in het beveiligen. Het bestuursorgaan heeft dan in het geheel geen regie over de situatie en voldoet dan niet aan de regelgeving. Dat probleem is wel bekend, maar niet snel op te lossen. Het zelf voldoen aan de BIR en de BIG en het slagen voor de DigiD-audits is al een zodanige aanslag op de capaciteit, dat extra taken het overvragen van de organisatie is.

Intern leunen veel organisaties op de BIG of de BIR. Voor specifieke problematieken wordt gebruik gemaakt van specifieke oplossingen. Daarbij komt een aantal methodieken van het Centrum voor Informatiebeveiliging en Privacybescherming voorbij onder de naam Grip op Privacy. Deze bieden een raamwerk om organisaties te helpen met het voldoen aan de Wbp. Ook het maken van risicoanalyses als basis voor beleidsvoorstellen komt regelmatig voorbij.

Deze benadering lijkt hoogdravend, maar in de praktijk gaat het ook gepaard met het regelen van vaak nog hele basale zaken. In veel organisaties is er veel achterstand met het up-to-date krijgen van software. Er is veel achterstallig onderhoud te verrichten met het uitfaseren van niet meer ondersteunde softwareversies, waarvoor projecten moeten worden gestart. Een populaire stap ‘omdat deze makkelijk met het argument compliance is te verkopen’. En ‘de kosten voor de reguliere ICT-afdeling komen niet op het beveiligingsbudget’.

Ook is bij diverse organisaties het maken van backups opnieuw onder de aandacht gekomen nu ransomware een groeiend probleem is. Wie daardoor wordt getroffen moet in ieder geval melding doen bij de Autoriteit Persoonsgegevens en dat trekt aandacht. Door te werken met goede reservekopieën is er een andere oplossing dan op de chantage in te gaan. De Autoriteit Persoonsgegevens is er klip en klaar over: een ransomware aanval is een datalek, backup of niet. “De verantwoordelijke kan er bij ransom- of cryptoware niet van uitgaan dat de inbreuk beperkt is gebleven tot het zichtbaar besmette bestand of systeem. De besmetting kan het hele systeem en alle gekoppelde bestanden raken”, schrijft de organisatie zelf.

Bewustwording

Een andere belangrijke poot in het uitrollen van een beveiligingsstrategie is volgens de CISO’s het inzetten op bewustwording. Die stap is belangrijk, omdat in de Wbp niet alleen over technische maatregelen wordt gesproken maar ook over organisatorische maatregelen. Een groot gedeelte van de beveiliging van persoonsgegevens leunt op het gedrag van medewerkers en het inzetten op goede procedures. Daarom gaat een deel van de energie op aan het goed voorlichten van mensen.

Daarbij is de drijvende kracht niet alleen de huidige Nederlandse wetgeving, maar ook de Algemene Verordening Gegevensbescherming. Als in 2018 daadwerkelijk aan die regelgeving moet worden voldaan moeten organisaties een grote slag hebben geslagen. Zo moet bijvoorbeeld bekend zijn welke gegevens worden verwerkt en moeten bestuursorganen dat ook kunnen oplepelen. Het zoeken naar inzicht in die gegevens brengt veel nieuwe risico’s op de radar en voedt daarmee de beveiligingsplannen.

Andere beveiligingsdoelen

Bij het maken van beveiligingsplannen lopen de doelen van een bestuur niet synchroon met de wensen van de wetgever. Bij bijvoorbeeld gemeenten spelen naast het voorkomen dat persoonsgegevens bij de verkeerde mensen kunnen terechtkomen, verloren gaan of onrechtmatig worden verwerkt, ook andere problematieken een rol. Zo moet dienstverlening worden gewaarborgd en de nodige systemen daarvoor beschikbaar zijn, administraties correct zijn en de vertrouwelijkheid van bepaalde bestuurlijke documenten worden gewaarborgd. De nervositeit over kritische vragen in de raad is dan groot. De Wbp wedijvert dan ook met andere eisen, die politiek zijn en voor het gevoel van de CISO’s net zo zwaar wegen.

De IBD ziet wel veel aandacht voor beveiliging, als het om de Wbp gaat. “Het is nu duidelijker dan ooit waar organisaties en dus ook gemeenten voor staan en aan moeten voldoen om de privacy te waarborgen. Zeker door de toename van informatiestromen binnen gemeenten, onder andere door de samenwerking in ketens, is de gemeente kwetsbaarder geworden. Informatiebeveiliging heeft prioriteit gekregen. Alhoewel, hier wat meer, daar wat minder”, vertelt Efstratiades. In de ondersteuning werkt de organisatie dan ook aan een programma dat zich toespitst op de specifieke situatie voor gemeenten op de verschillende aspecten van privacy.

Angst voeden

Die angst voor het op de vingers worden getikt, wordt ook gevoed door de toezichthouder. Een goed voorbeeld is een onderzoek uit april 2016. Daarin concludeerde de Autoriteit Persoonsgegevens dat gemeenten onzorgvuldig met gegevens omgaan. Uit het onderzoek blijkt dat de gemeente bij het verwerken van gegevens voor voorzieningen in het sociaal domein de aanvrager ook toestemming voor verwerking vraagt – iets wat moeilijk is te weigeren. Maar volgens de AP kan dat niet, want die gemeenten hebben geen goed overzicht van de doelen, grondslagen en persoonsgegevens die zij verwerken binnen de rechtsgronden van de diverse verschillende wetten in het sociaal domein. Zij voldoen dus al snel niet aan de randwoorwaarden van de Wbp.

De wetenschap dat het haast onmogelijk is om onder de huidige omstandigheden volledig aan de Wbp te voldoen, maakt het praten over de beveiliging voor de CISO’s ingewikkeld. “Niemand wil met zo’n boodschap in de media naar buiten treden”, stelt Efstratiades en CISO’s en de overigen bevestigen dat desgevraagd. “Het gevolg is dan niet moeilijk om te bedenken”, licht er een toe. “Mijn aandacht is er vooral op gericht om zo snel mogelijk compliant te zijn en dat is niet automatisch hetzelfde als veilig zijn.”

Dat laatste is ook een verhaal van mensen en middelen. Er wordt vooral erg operationeel gewerkt; zaken als bijvoorbeeld de communicatie op orde krijgen heeft op dit moment weinig prioriteit. De slag om budgetten wordt iets gemakkelijker nu de Cybersecurityraad adviseert om tien procent van het ICT-budget te steken in beveiliging en door de druk van de wetgever. Maar in de kern blijft bij beveiliging de focus liggen op achterstallig onderhoud verrichten, leunen op de kennis en kunde van de leverancier en het introduceren van normenkaders. En, zoals een CISO toevoegt: “hopen dat je ondertussen niet getroffen wordt door een datalek.”

Ik probeer zo snel mogelijk compliant te zijn en dat is niet automatisch hetzelfde als veilig zijn

Brandweer wil data slimmer combineren

De vierde industriële revolutie omvat technologische ontwikkelingen in brede zin en gaat razendsnel. Met als gevolg dat de omgeving verandert. Om de brandveiligheid te kunnen blijven waarborgen heeft de brandweer behoefte aan een kwaliteitssysteem om relevante data slimmer te kunnen combineren.

Barry van 't Padje is de informatiemanager van Brandweer Amsterdam Amstelland. "Ik ben van de vraagkant", zegt hij over zijn functie. "Welke mogelijkheden ontstaan er door de vierde industriële revolutie? Hoe werken we, wat zijn onze doelen en hoe willen we die realiseren?"

"Technologie gaat steeds dichter op je huid zitten", ziet Barry. "Je zintuigen maken steeds meer gebruik van digitale middelen. De brandweer heeft behoefte aan een spiegel van de omgeving, gezien vanuit het perspectief van fysieke veiligheid. Welke digitale feiten zijn voor ons op welke momenten van belang en met wat voor soort interfaces kunnen we deze op een slimme manier gebruiken? We moeten gelijke tred zien te houden met de ontwikkelingen."

Als de brandweer uitrukt, is informatie over het incident en haar omgeving nodig. "Er zijn op dat moment best veel relevante (sensor-)data beschikbaar. Maar wij hebben nog maar heel beperkt toegang tot die data", stelt Barry. "Er zijn bijvoorbeeld duizenden brandmeldpanelen in onze regio, maar die zijn niet

Barry van 't Padje

'open'. We moeten nog steeds fysiek naar het paneel om de informatie te verkrijgen. Dat kan echt handiger. Hetzelfde geldt voor camerabeelden of social media-berichten. Onze infrastructuur is nog niet voldoende aangesloten op de mogelijkheden."

Besef rond big data moet nog komen

De infrastructuur heeft naast technische ook juridische aspecten. "Het is voor ons bijvoorbeeld belangrijk om tijdens een brand te weten of de bewoners verminderd of niet zelfredzaam zijn, of wellicht gevaarlijk. Dit zijn persoonsgegevens, en daarom moeten we goed nadenken over hoe we met de privacy van betrokkenen willen omgaan. De privacywetgeving werkt in de praktijk vaak als een verbod en de procedures die het gebruik van gegevens regelen schrikken enorm af. Maar ik denk dat er veel situaties zijn waarin mensen bereid zijn persoonsgegevens te delen. Tijdens een levensbedreigende situatie is dat echt geen issue. We moeten bedenken hoe we dit makkelijker kunnen maken."

Risicoprofielen

"Eén van de belangrijkste toegevoegde waardes van big data voor de brandweer is de mogelijkheid om nauwkeurige risicoprofielen op te stellen". vervolgt Barry. "De risico's zijn namelijk bepalend voor welke producten en diensten de brandweer moet aanbieden. Hoe groter het risico, hoe meer veiligheidsmaatregelen nodig zijn, van preventief tot repressief. Tot nu toe werden deze risico's grofmazig op basis van ervaring en vakkennis in kaart gebracht. Door de beschikbaarheid van grote hoeveelheden data kunnen deze risico's veel beter worden geïnventariseerd en ontstaat ook de mogelijkheid om de effecten van de veiligheidsmaatregelen te meten. Er ontstaat, met andere woorden, de mogelijkheid van een evidence based praktijk. Als we het goed aanpakken, gaat ons leervermogen met sprongen vooruit."

Een belangrijk onderwerp daarbij is de verhouding tussen preventief en repressief. "In de toekomst zal de informatievoorziening veel meer naar de voorkant gaan. Stedenblokken branden niet meer af, zoals vroeger. Laat staan een hele wijk. Gebouwen worden tegenwoordig heel anders gemaakt. De focus verschuift steeds meer van de repressieve kant naar de niet-repressieve kant: hoe voorkom je een incident? Hoe kun je een veilige omgeving creëren? Als ook dit op een goede manier

Informatie wordt steeds meer een productiefactor

digitaal wordt vastgelegd, kan er een vruchtbare wisselwerking met de repressieve kant ontstaan. Dat noemen wij ketengericht werken."

Nadenken over goed informatiesysteem

"Al deze ontwikkelingen maken informatiegestuurd werken binnen de brandweer steeds belangrijker," voorspelt Barry. "Informatie wordt steeds meer een productiefactor. Je moet daarom nadenken over hoe je een kwalitatief hoogwaardig informatiesysteem opzet. Hoe moet je testen? Hoe moet je je functioneel beheer inrichten? Welke informatie heb je specifiek nodig om je werk goed te kunnen doen? Voor dit soort vraagstukken hebben we SYSQA ingeschakeld. Zij zijn goed in het ontwikkelen van kwaliteitssystemen."

"In welk systeem de data is opgeslagen is feitelijk niet belangrijk, als het maar in een netwerk past en je erbij kunt. Maar we moeten wel naar nieuwe wegen zoeken waarmee we die enorme hoeveelheid beschikbare data kunnen opslaan en combineren. En we moeten nadenken over de juridische en beleidsmatige fundamenten waarmee dit op een verantwoorde manier kan."

Aftellen naar de Algemene Verordening Gegevensbescherming (AVG):

Huiswerk!

Per 25 mei 2018 is de nieuwe Europese privacywetgeving van toepassing in alle lidstaten. Dat geeft bestuurders nog ruim een jaar om zich goed voor te bereiden. Wat gaat er in juridische zin voor overheden veranderen en wat zijn daarbij de aandachtspunten?

Fred Teunissen

Televisieschermen en geluidsboxen, die conversaties in de kamer opvangen en doorsturen naar 'de Centrale', smart meters die de kleinste nuances in het energiegebruik in uw woning vastleggen, social media die niet alleen een reeks persoonsgegevens registreren, maar – op basis van uw surfgedrag – ook uw interessegebieden, politieke voor- en afkeuren, seksuele gerichtheid en aanwijzingen voor uw fysieke gesteldheid en dat alles samenbrengen in diepgravende persoonlijke profielen. Het zijn maar drie voorbeelden van de oprukkende digitale techniek en een privacy die daardoor stevig onder druk komt te staan. Door de digitale revolutie verandert ook ons denken over privacy. We worden er langzaam maar zeker wat soepeler in.

Versoepeling

De wetgeving versoepelt mee, althans op sommige punten. Nu is het nog zo dat u al uw privacygevoelige gegevensbewerkingen moet melden bij de Autoriteit Persoonsgegevens. Dit is vastgelegd in de Wet bescherming persoonsgegevens (Wbp) uit 1995. Onder de nieuwe Europa-brede Algemene Verordening Gegevensbescherming (AVG) hoeft dit niet meer. Voortaan bent u namelijk uw eigen waakhond. U dient straks te kunnen aantonen dat u uw datazaakjes goed geregeld heeft. Dit is vastgelegd in de zogeheten documentatieplicht. U moet hard kunnen maken dat uw processen *privacy by design* volgen, dan wel *privacy by default*. Dit laatste houdt in dat u niet meer gegevens mag vragen dan strikt noodzakelijk is. Uw vinkjes moeten voortaan standaard uit staan.

Op andere punten is de AVG een stuk strakker. Als overheidsorganisatie bent u volgens de AVG verplicht een PIA (privacy impact assessment) uit te (laten) voeren. En u moet een Functionaris Gegevensbescherming (FG) aanstellen als u die al niet had. Ook kleine overheden krijgen met deze verplichting te maken. En nog een verschil: datalekken moet u voortaan altijd melden. Er zijn geen uitzonderingen meer.

Dit zijn een paar belangrijke verschuivingen. Hoe ingrijpend zijn ze, vergeleken met de situatie sinds 1995?

Data mapping

Gerrit-Jan Zwenne, hoogleraar recht en de informatiemaatschappij bij de afdeling eLaw van de Universiteit Leiden, verwacht geen grote verschuivingen als gevolg van de invoering van de nieuwe Europese Wet. Hij schat dat 80 procent ongeveer hetzelfde zal zijn vergeleken met de Wbp, maar dan wel een stuk gedetailleerder en meer omvattend. "Er is tot op zekere hoogte sprake van codificatie. Er is inmiddels de nodige jurisprudentie gekomen. Ook hebben de toezichthouders nu ruime ervaring opgedaan met de huidige regelgeving. Er is daardoor een scherper beeld ontstaan en consensus over wat onder de privacywetgeving valt en wat niet."

In de 20 procent die het verschil uitmaakt, ruimt Zwenne een prominente plaats in voor *accountability*. "Daar ligt nu veel meer nadruk op. Je moet kunnen aantonen dat je voldoet aan wat in de Verordening staat. Om dat te kunnen, moet je precies weten welke gegevensverzamelingen je waar in je organisatie hebt en voor welke doelen je de gegevens inzet. Op dit moment hebben te veel overheden daar een te onbepaald beeld van."

Zwenne wijst in dit verband op het feit dat de Autoriteit Persoonsgegevens onlangs enkele gemeenten op de vingers tikte,

Toezichthouders bewegen zich langzaam maar zeker af van strikte doelbinding

omdat ze niet wisten wat ze aan gegevensbronnen in huis hadden. "In de AVG is een strenge documentatieplicht opgenomen. Je moet bijvoorbeeld logfiles bijhouden, dus vastleggen wie op welk moment bij welke gegevens is geweest. De organisatie van je informatievoorziening moet daarop wel zijn ingericht. Op dit punt moet nog heel wat werk worden verzet door overheden."

Zwenne raadt aan om de tijdspanne tot aan het van kracht

worden van de AVG vooral te benutten voor *data mapping*. "Daar zijn tal van goede tools voor. Elke accountantsorganisatie of privacyadviesbureau kan je daarover voorlichten."

En dan is er nog de aanstelling van een FG. "Bij de Rijksoverheid en de grote gemeenten zijn al zulke functionarissen aangesteld," verduidelijkt hij, "maar nog niet op de overige niveaus. Ook kleine overheden zijn hiertoe volgens de AVG verplicht. Zij zijn daar vaak niet op ingericht en kunnen ervoor kiezen om deze taak uit te besteden aan een dienstverlenend bedrijf, maar ik vraag me af of dat wel zo verstandig is. Als gegevensverwerking tot je kerntaken behoort – en bij overheden is dat altijd het geval – dan is er veel voor te zeggen om de expertise op het punt van privacy in eigen huis te houden."

Bezinning

Belangrijke peiler in zowel de Wbp als de AVG is de zogeheten doelbinding. *Datagraaien* mag nog steeds niet. Dit houdt in dat het doel waarvoor de gegevens worden verzameld, vastgelegd en verwerkt duidelijk omschreven moet zijn. Dat is logisch, want dat maakt deze activiteit 'tastbaar' en daarmee in principe controleerbaar. Maar daarmee loopt de AVG wel enigszins achter bij de maatschappelijke realiteit van big data-toepassingen. De kern van echt innovatieve big data is nu juist dat er geen nauw omschreven doel is, omdat dit pas 'tijdens de rit' contouren krijgt.

De overheid is een monopolist. Je kunt als burger als iets je niet zint niet naar een andere overheid overstappen

Corien Prins, hoogleraar Recht en Informatisering aan de Universiteit van Tilburg, beaamt dat de AVG op dit punt nog voor zijn inwerkingtreding al achter de feiten aanloopt. "Je ziet in de praktijk nu al dat er een verschuiving optreedt. Toezichthouders bewegen zich een beetje af van die strikte doelbinding." Tegelijkertijd treedt het begrip 'gerechtvaardigd belang' meer op de voorgrond, aldus Prins. "Onder de huidige Wbp is verantwoording afleggen over de keuzes die organisaties maken in het verwerken van persoonsgegevens een minder expliciete opdracht. Dat is volgens de nieuwe AVG wel het geval. Het effect hiervan kan zijn dat wat vroeger gedacht werd wel te kunnen, omdat er voorafgaand aan de verwerking minder expliciet om verantwoording afleggen werd gevraagd, nu niet meer mag, bijvoorbeeld omdat het gerechtvaardigd belang niet goed kan worden gemotiveerd. En omgekeerd, dat wat vroeger niet mocht omdat het doel niet goed was omschreven, nu wel mag, omdat er een evident gerechtvaardigd en goed gemotiveerd belang mee is gediend."

Prins raadt overheden aan om de verplichte PIA's aan te grijpen voor een bezinning op precies deze vraagstukken: is er wel een voldoende gerechtvaardigd belang? "Zo'n PIA kan als resultaat opleveren dat je van voorgenomen activiteiten afziet. Overheden kunnen dit instrument gebruiken om in sommige gevallen duidelijk NEE te zeggen tegen eerder door hen geformuleerde beleidsintenties."

Waarborgen

En de burger? Gaat de rechtspositie van de Europese burger erop vooruit? "Dat verwacht ik wel," reageert Zwenne, "maar we moeten ons ook niet rijk rekenen." Als voorbeeld noemt hij het klachtrecht. "Onder de Wbp heb je ook een klachtrecht, maar de AP hoefde niet iets met zo'n klacht te doen. Ze konden hem voor kennisgeving aannemen of volstaan met een beleefd antwoordbriefje: 'we hebben uw signaal ontvangen'. In de nieuwe situatie is dat niet meer vanzelfsprekend. De AP zal dan al snel aantoonbaar actie moeten ondernemen."

Corien Prins is minder optimistisch gestemd over de positie van de burger. "De overheid is een monopolist. Je kunt als burger als iets je niet zint niet naar een andere overheid overstappen. De overheid heeft zo enorm veel macht. Daarom zouden er wat mij betreft betere wettelijke waarborgen ingebouwd moeten worden."

Ze geeft het voorbeeld van het onderscheid in de AVG tussen gewone en bijzondere gegevens. "Dat onderscheid kun je zo eigenlijk niet meer maken. Iedereen weet dat je door de combinatie van twee of meer gewone gegevens bijzondere, soms zelfs uiterst gevoelige gegevens kunt creëren. Overigens is het wel zo dat de AVG alleen het nieuwe juridische raamwerk omvat. De nationale parlementen moeten nu voor het verwerken van bepaalde gegevens – bijvoorbeeld gezondheidsgegevens – nadere regels uitwerken. En bij die gelegenheid zijn er voor die verwerkingen nog volop kansen om in de dagelijkse praktijk van de regelgeving betere waarborgen aan te brengen."

Met iedere combinatie van datastromen worden persoonlijke gegevens uitgebreid en het beveiligingsrisico vergroot. Maak privacy onderdeel van het gewenste eindresultaat en gebruik bewezen privacy- of securityoplossingen van derden.

Maak van veilige software een harde eis

In oktober van dit jaar lagen de gegevens op straat van 412 miljoen gebruikers van datingbedrijf FriendFinder. Het ging onder andere om gebruikersnamen, wachtwoorden, e-mailadressen en IP-adressen. Dat was op zich al erg genoeg, maar FriendFinder host ook 'datingsites' voor mensen die op zoek zijn naar porno en (buitenechtelijke) seks. Dit zijn diensten waar gebruikers over het algemeen privé gebruik van willen maken en de openbare persoonsgegevens zijn daarmee een bron van chantage. Iedereen kan zich voorstellen wat een impact dit kan hebben op levens en loopbanen. Voorvallen als deze dragen bij aan de groeiende realisatie dat databeveiliging een zeer serieuze kwestie is voor iedereen.

Alles is data

Op het moment van schrijven is de Friendfinder-hack een van de grootste datalekken in de geschiedenis, maar dat zal niet zo blijven. "Datalekken zijn een feit", zegt Brenda Langedijk, security consultant voor SIG (Software Improvement Group). "De wereld draait op software en software is kwetsbaar voor aanvallen van buitenaf en slordigheid van binnenuit. Wat voor bedrijf je ook bent, software is jouw business geworden." Naast berichtgeving in de media, groeide dat besef ook door het aanscherpen van de wetgeving, de Europese General Data Protection Regulation (GDPR) en Wet Meldplicht Datalekken. De verhoging van boetes heeft menig bestuurder opgeschrikt en de vaak verplichte aanstelling van een functionaris voor de gegevensbescherming (FG) dwingt organisaties tot zelfonderzoek naar hoe hun software met data omgaat. Langedijk: "Het speelkwartier is voorbij. Na 25 mei 2018 gaan de boetes uitgedeeld worden en ze zijn beslist fors. Aan het eind van de rit bestaat de kans dat de bestuurder ook persoonlijk aansprakelijk wordt gehouden."

Privacy by design

Maar waar te beginnen? "Wij pleiten voor privacy by design, softwareontwikkeling met privacy erin gebakken", zegt business consultant Cathal Boogerd van SIG. Met schone lei beginnen wil natuurlijk iedereen, maar wat te doen met digitaal erfgoed? "Legacy maakt het lastiger. Decennia aan data worden opnieuw of anders ontsloten, bijvoorbeeld door nieuwe software. Met iedere combinatie van datastromen worden persoonlijke gegevens uitgebreid en het beveiligingsrisico vergroot. Daarom moet voorafgaand aan ieder veranderingsproces privacy worden meegenomen in het gewenste eindresultaat. Maak het een eis en toets daarop, dan komt het in de software wel terecht."

Minimaal de wet

Langedijk merkt in de markt nog steeds verwarring over wat wel en niet mag als het gaat om persoonsgegevens. "Instinctief weten we het wel. Waarom dan toch digitaal laten rondslingeren wat je niet op een bureau zou laten liggen? Er is een niveau waar je niet onder mag zitten en dat is de wet. Zorg dat bestaande richtlijnen en regelgeving worden vertaald naar concrete richtlijnen voor de eigen organisatie. Houd voor ogen dat hoe meer data je bewerkt, hoe meer risico je creëert." Langedijk adviseert om gebruik te maken van bestaande 'privacy enhancing technology' (PET). "We zien nog regelmatig software waarin ontwikkelaars zelf een gemankeerde oplossing hebben bedacht voor security of privacy. Ons uitgangspunt is: ga niet zelf bouwen, er is voldoende technologie beschikbaar met bewezen security- en privacy-eigenschappen waarmee je je bovendien de onderhoudslast bespaart. Denk bijvoorbeeld aan de encryptie die WhatsApp gebruikt. Waarom zou je zelf nog gaan sleutelen?" Het slotadvies van SIG: behandel persoonsgegevens als een explosieve stof die door verkeerd gebruik of blootstelling aan de buitenlucht tot grote schade kan leiden. Niet alleen voor degene die het hanteert, maar ook voor de directe omgeving.

Vijf slechte gewoonten om te breken (privacy-antipatterns)

AGGREGATE_LATE: het verzamelen van meerdere privacygevoelige informatiebronnen en die opslaan om later op te tellen. Bijvoorbeeld het gemiddeld aantal gebruikers per uur. Waarom gebruikersdata bewaren met bezoektijden en later optellen? Beter is het meteen te tellen en de gebruikersgegevens weg te gooien.

ASK_TOO_MUCH: alle gegevens van een persoon opvragen in een app of op een website omdat het vast nog eens van pas kan komen. Al die data kunnen gaan lekken en dat komt helemaal niet van pas. Minimaliseer. Vraag alleen wat nodig is (een game hoeft toch ook geen toegang tot adresboek en locatie?)

KEEP_TOO_LONG: onnodig lang bewaren van gegevens. Gooi daadwerkelijk weg wat niet meer nodig is of wat niet langer wettelijk verplicht is om te bewaren. FriendFinder bleek bijvoorbeeld twintig jaar aan data te hebben opgeslagen – en gelekt. Waarom?

SCATTER_DATA: persoonlijke gegevens op verschillende plekken bewaren zonder dat bij te houden. Alleen na inventarisatie komen risico's in beeld, kunnen ze geminimaliseerd worden en is het mogelijk om gegevens van personen echt te verwijderen of te corrigeren.

TRUST_ALL_FRIENDS: iedereen in de organisatie mag alle gegevens zien. Dat is weliswaar eenvoudig in gebruik en beheer, maar het is beter om hier grenzen te stellen vanwege privacyrisico's.

Scanauto in Amsterdam. Jaap-Henk Hoepman: “Rechters wegen bij hun uitspraken de proportionaliteit en subsidiariteit. Is het bijvoorbeeld nog nodig dat gemeenten alle nummerborden inscannen voor parkeerheffingen?”

Technische implicaties van de AVG

Privacy by Design

Met de komst van strengere Europese regelgeving dringt bij organisaties het besef door dat ze ‘iets met privacy’ moeten in hun digitale bedrijfssystemen. Maar hoe bed je privacy op een fundamentele manier in het ontwerp van gegevensverwerkingen in? “Het is meer informatiekunde dan informatica.”

Fred van der Molen

In een wereld waarin burgers met een druk op AKKOORD toestaan dat de Facebooks en Googles van deze wereld meer persoonlijke gegevens naar binnen slurpen dan bedrijven ooit eerder deden, lijkt privacy een concept uit een romantisch verleden. Tegelijkertijd voeren politici en privacyorganisaties strijd om de digitale privacy van burgers beter te waarborgen. En is – dankzij Europa, jawel – de Algemene Verordening Gegevensbescherming (AVG) aangenomen die strengere regels en hogere boetes belooft dan nu gelden. Wordt hier een achterhoedegevecht gevoerd, of komt dankzij de AVG het onderwerp digitale privacy werkelijk hoger op de agenda te staan van bedrijven en overheidsorganisaties? En daarmee op het bordje van systeemarchitecten, informatici en applicatiebouwers?

Dat laatste lijkt het geval, gelet op de stroom publicaties, blogs en congressen over onderwerpen als ‘privacy by design’ en andere aspecten die voortvloeien uit de AVG. De nieuwe verordening treedt op 25 mei 2018 in werking. Ondertussen oriënteren meer en meer organisaties zich op hoe ze AVG-compliant kunnen worden. Wie met persoonsgegevens werkte, overtrad wellicht al de Wet Bescherming Persoonsgegevens (WBP), maar de risico’s om niets te doen lijken groter te worden.

“De maximale boetes kunnen enkele procenten van de bruto wereldwijde jaaromzet bedragen. Dat maakt privacy in ieder geval voor bedrijven een onderwerp in de bestuurskamer”, stelt wetenschapper Jaap-Henk Hoepman van de Rijksuniversiteit Nijmegen.

“Dat je er iets mee moet, is duidelijk. Maar wat? Er is grote onzekerheid in de markt”, aldus consultant Rob van der Veer van de Software Improvement Group (SIG). “Want hoe heet wordt de soep uiteindelijk gegeten? Daarvoor is het toch wachten op hoe de wet daadwerkelijk wordt toegepast.”

Raamwerk

Maar voordat de eerste processen worden gevoerd, proberen kennisinstellingen de organisatorische en technische implicaties van de nieuwe regelgeving in kaart te brengen. Eén daarvan is TNO, die onder de naam RESPECT4U een ‘privacyraamwerk’ in ontwikkeling heeft. TNO-onderzoeker Marc van Lieshout over de achtergrond: “Met de AVG is er een wettelijk kader waarin de rechten van het individu en plichten voor organisaties worden benoemd. Maar er staan veel open normen in, bijvoorbeeld rond privacy by design. Wat betekent dat nu precies in de praktijk? We willen met dat raamwerk geen checklist voor goed gedrag afleveren, maar wel een hulpmiddel om organisaties in staat te stellen om te doen wat ze willen doen, met een goed oog voor de privacy-aspecten.”

Van Lieshout wijst er ook op dat het met het benoemen van rechten van het individu niet klaar is. “Je kunt moeilijk verwachten dat gewone burgers zich daar op elk moment in gaan verdiepen. Wij gebruiken graag de vergelijking met voedselkwaliteit. Gebruikers kunnen en willen niet alles zelf controleren. Ze vertrouwen erop dat producten die in de winkel liggen aan normen van voedselveiligheid voldoen. Vergelijkbaar zouden we ook op het gebied van privacy keuringsinstanties en kwaliteitslabels willen hebben.”

Van Lieshout en Hoepman (RU) zitten in de directie van het Privacy & Identity Lab (PI.lab), een platform waarin TNO en de

universiteiten van Nijmegen en Tilburg samenwerken aan kennisopbouw rond de juridische, organisatorische en technische aspecten van digitale privacy en identiteit.

Privacy by design

In de AVG wordt expliciet gesproken over 'privacy by design'. Hoepman: "Dat betekent dat je serieus moet gaan nadenken hoe je systemen privacyvriendelijk gaat ontwerpen. En dat je die vervolgens ook goed moet documenteren."

De belangstelling voor privacy onder systeemarchitecten en applicatiebouwers lijkt daarmee dezelfde weg te volgen als eerder die voor security: van negeren, via het implementeren van reparaties achteraf naar het integraal inbedden in het ontwerp. Met dit verschil dat organisaties sneller het nut inzien van beveiligingsmaatregelen. Hoepman: "Dat is wel een essentieel verschil. Bij privacykwesties is de organisatie die persoonlijke gegevens verzamelt enerzijds verantwoordelijk voor het beschermen ervan, maar heeft die aan de andere kant juist belang bij het verzamelen van die informatie. Heel plat gezegd: zonder privacy-beschermende wetgeving was er voor organisaties ook geen privacy-probleem. Dat ligt bij security wel anders. Daar valt de boze buitenwereld je aan."

Privacybeleid wordt dan ook vaak ervaren als een blok aan het been. Het is gedoe. Maar met boeteclausules in het vooruitzicht dringt het besef door dat negeren geen optie meer is. En omdat achteraf aanpassen lastiger en kostbaarder is dan meteen inbouwen, groeit de aandacht voor Privacy by Design.

Hoepman stelt vast dat er meer aandacht voor ontwerpstrategieën ontstaat, terwijl tot voor kort de meeste aandacht uitging naar technologieën om applicaties veiliger te maken, zoals identiteitscontrole en encryptie.

Hoepman: "Maar ik moet toegeven dat het onderwerp 'privacy by design' makkelijker ingang vindt bij juristen en organisatieadviseurs dan bij systeemarchitecten en techneuten. Die vinden het vaak een vaag onderwerp. Het is meer informatiekunde dan informatica."

In mei 2016 bracht het CIP (Centrum Informatiebeveiliging en Privacybescherming) een uitgebreide handleiding uit voor Privacy by Design, waarin de consequenties van de nieuwe privacy-regelgeving zijn uitgewerkt tot zeven ontwerpprincipes. De CIP Handleiding beoogt organisaties handvatten te geven voor de omgang met privacy bij het ontwerpen van gegevensverwerkingen.

Nog dichter op de praktijk staan de ontwerpstrategieën die Hoepman op zijn site deprivacycoach.nl noemt. Hij onderscheidt daarin data-georiënteerde en procesgeoriënteerde strategieën (zie kader). Tot de eerste categorie horen principes om de opslag en verwerking van persoonsgegevens zoveel mogelijk te minimaliseren, zo weinig mogelijk gegevens gecentraliseerd op te slaan en die zoveel mogelijk te anonimiseren.

Bij de procesgeoriënteerde strategieën draait het om de gebruiker: die moet altijd worden geïnformeerd en om toestemming gevraagd wanneer zijn persoonlijke gegevens worden opgeslagen. Bovendien moet die gebruiker gegevens kunnen corrigeren. Daarnaast dient de organisatie enerzijds intern een privacyvriendelijke verwerking af te dwingen en anderzijds zich daarover extern te verantwoorden.

RESPECT4U

Zoals gezegd ontwikkelt TNO een privacyraamwerk onder de naam RESPECT4U. RESPECT is een acroniem dat staat voor Responsible, Empowerment, Secure, Proactive, Ethical, Cost-benefits en Transparantie. Over elk van deze aspecten kan Van Lieshout snel een middag vullen. Maar hij wil in ieder geval als belangrijke boodschap meegeven dat organisaties privacy niet enkel als kostenpost moeten zien. "Als je het negatief benadert, kun je aanvoeren dat je met een goed digitaal privacybeleid boetes kunt vermijden. Maar transparantie en betrouwbaarheid zijn ook redenen waarom burgers liever met jouw organisatie in zee gaan. Wij denken dat het dezelfde rol gaat spelen als 'duurzaamheid' in de beslissing van burgers met wie ze in zee willen gaan."

SIG is een organisatie die zich specialiseert in het testen van softwarekwaliteit. Inmiddels deelt het bedrijf ook rapportcijfers uit voor de implementatie van privacy-aspecten. Van der Veer: "Privacy wordt vaak een onderwerp bij security-audits. Dan ga je vragen stellen bij gegevensstromen. Heb je al die gegevens nodig? Moet je ze wel centraal opslaan? Zijn ze wel actueel? Hoe lang worden ze bewaard? Organisaties zijn in eerste instantie terughoudend om daarop in te gaan. Ze vrezen ook wat er uitkomt en de verplichtingen die dat met zich meebrengt."

Maar de nieuwe wetgeving en de dreigende boetes zet het thema wel prominenter op de agenda. "Wij beschouwen het in ieder geval als een belangrijk nieuw speerpunt om organisaties daarbij te ondersteunen."

Conflicterende belangen

Het bedrijfsmodel van social mediabedrijven is voor een groot deel gebaseerd op het verzamelen van zoveel mogelijk persoonskenmerken. Privacy-beperkingen zijn dan vooral hinderlijk. Maar ook overheidsorganisaties zijn gretige verzamelaars. Zo vlooit de fiscus parkeergegevens van alle Nederlanders door om te controleren of leaserijders hun bedrijfswagen toch niet meer privé gebruiken dan ze opgeven. En de gegevens die bedrijven als Bluetraffic en CityTraffic leveren op basis van wifi- en bluetooth tracking van mobiele telefoons worden niet alleen door winkelketens benut maar ook door gemeenten. Je kunt zo handig bezoekersaantallen en -stromen in kaart brengen. De Autoriteit Persoonsgegevens heeft in een concreet geval bepaald dat deze methode in strijd is met de Wet bescherming persoonsgegevens (Wbp) en beperkingen opgelegd in combinatie met een dwangsom.

Hoepman: "Rechters wegen bij hun uitspraken de proportionaliteit en subsidiariteit van de gegevensverzameling. Is het bijvoorbeeld nodig dat gemeenten alle nummerborden inscannen voor parkeerheffingen? Nu kan het antwoord positief zijn, maar zodra iemand iets bedenkt waardoor de heffing ook efficiënt op een meer privacyvriendelijke manier kan worden geregeld, ben je eigenlijk verplicht dat te implementeren. De stand van de techniek kan dus dwingen tot herijking van een bepaalde werkwijze."

Meer informatie: www.pilab.nl, www.cip-overheid.nl

Acht privacy-ontwerpstrategieën

DATA-GEORIËNTEERDE STRATEGIEËN

Minimaliseer: beperk zo veel mogelijk de verwerking van persoonsgegevens. Selecteer alleen relevante personen of gegevens. Verwijder persoonsgegevens zodra ze niet langer nodig zijn.

Scheid: scheid persoonsgegevens zo veel mogelijk van elkaar. Verzamel persoonsgegevens in verschillende databases. Distribueer de verwerking over verschillende locaties. Doe zoveel mogelijk in de apparatuur van de eindgebruiker.

Abstraheer: beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt. Aggregeer informatie over categorieën personen in plaats van ieder individu. Vat gedetailleerde informatie samen in meer algemene gegevens.

Bescherm/maak onherleidbaar: voorkom dat persoonsgegevens openbaar worden. Beperk toegang tot en beveilig persoonsgegevens. Verbreek de link tussen personen en hun gegevens. Maak data onherleidbaar, bijvoorbeeld door deze te mixen of te anonimiseren.

PROCES-GEORIËNTEERDE STRATEGIEËN

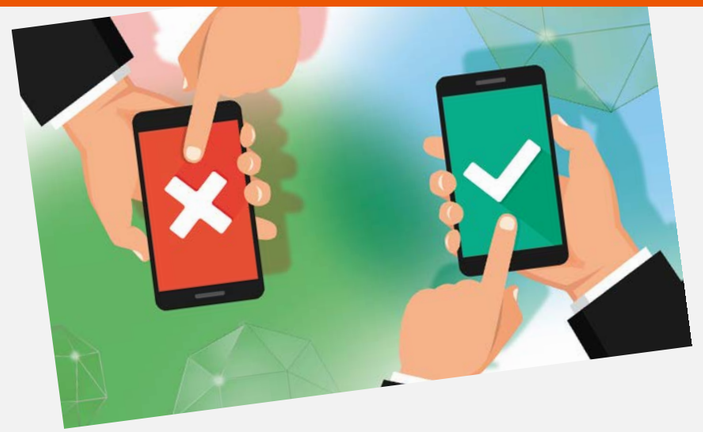
Informeer: informeer gebruikers op een begrijpelijke manier over de verwerking van hun persoonsgegevens. Waarschuw gebruikers als hun persoonsgegevens worden gebruikt, of als deze zijn gelekt.

Geef controle: geef gebruikers controle over de verwerking van hun persoonsgegevens. Vraag om toestemming. Geef de mogelijkheid om persoonsgegevens te corrigeren of te (laten) verwijderen.

Dwing af: committeer je aan een privacyvriendelijke verwerking van persoonsgegevens. Stel een privacybeleid op, en dwing deze af met technische en organisatorische maatregelen. Beleg verantwoordelijkheden. Controleer de implementatie van het beleid regelmatig.

Toon aan: toon aan dat je op een privacyvriendelijke wijze werkt. Verzamel logs en doe audits. Rapporteer de resultaten. Laat je certificeren.

Bron: www.deprivacycoach.nl (Jaap-Henk Hoepman).



Veilige Tweede Kamerverkiezingen vanuit de cloud

Het is essentieel dat bij de komende verkiezingen de data van uitslagen en opkomstpercentages optimaal beveiligd zijn. Dit zijn misschien wel de meest gevoelige data die een gemeente kan hebben. Kan een goede beveiliging ook in de cloud? Specialist PROCURA ontwikkelde een cloud-oplossing waarmee gemeenten verkiezingen vlekkeloos kunnen organiseren.

Van stempassen, stemhokjes, formulieren en drukwerk tot software. PROCURA levert aan meer dan driehonderd Nederlandse gemeenten alles voor de komende Tweede Kamerverkiezingen. Verantwoordelijk werk waarbij betrouwbaarheid essentieel is. Met een bijzondere cloud-oplossing biedt het bedrijf zijn verkiezingssoftware nu veilig en betrouwbaar aan. Arnoud Korten is manager Implementatie en Consultancy bij PROCURA. Hij vindt de keuze voor een cloudbased applicatie een logische. “Klanten verwachten nu eenmaal de flexibiliteit en efficiëntie die software uit de cloud mogelijk maakt. Wij willen op onze beurt klaar zijn voor de toekomst. Steeds meer applicaties waar wij gebruik van maken, gaan over naar de cloud. Om daar goed mee te kunnen blijven werken, moeten we zelf ook die overgang maken.” Tijdens de Tweede Kamerverkiezingen, kunnen de Nederlandse gemeenten gebruikmaken van het nieuwe softwarepakket PROCURA Verkiezingen. Ook dit pakket biedt PROCURA aan via een cloud-omgeving. PROCURA Verkiezingen is de opvolger van PROCURA’s Integraal Stem Systeem (ISS). Een pakket dat veel gemeenten jarenlang gebruikten om verkiezingen binnen hun gemeente in goede banen te leiden.

Gevoelige informatie

De keuze om PROCURA Verkiezingen vanuit de cloud aan te bieden, is volgens Korten ook een keuze voor veiligheid. “Zowel gemeenten als PROCURA willen de beveiliging van gegevens goed verzorgen. PROCURA Verkiezingen is een zeer uitgebreide projectplanningstool. Je legt erin vast wie welke stemlokalen bemant, wat de vergoedingen zijn, welke materialen er nodig zijn, maar ook wat de uitslag en opkomst is. Al met al bevat de software behoorlijk wat gevoelige informatie. Het is informatie die je koste wat kost uit de verkeerde handen wil houden.” Daar is het hoogste beveiligingsniveau nodig. Gemeentelijke dienstverlening moet voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). “Die vereist dat we de informatiebeveiliging tot in de puntjes regelen. Maar ook beschikbaarheid is voor ons belangrijk. Het is natuurlijk essentieel dat de software het tijdens de verkiezingen doet. Het móet gewoon werken.” Ook de schaalbaarheid en mogelijkheid updates en patches snel uit te rollen, is een voordeel van de overgang naar een cloud-based applicatie. Zo is de verwachting dat PROCURA Verkiezingen in de nabije toekomst wordt uitgebreid met apps en kandidaatstellingsmodules die het pakket steeds completer maken.

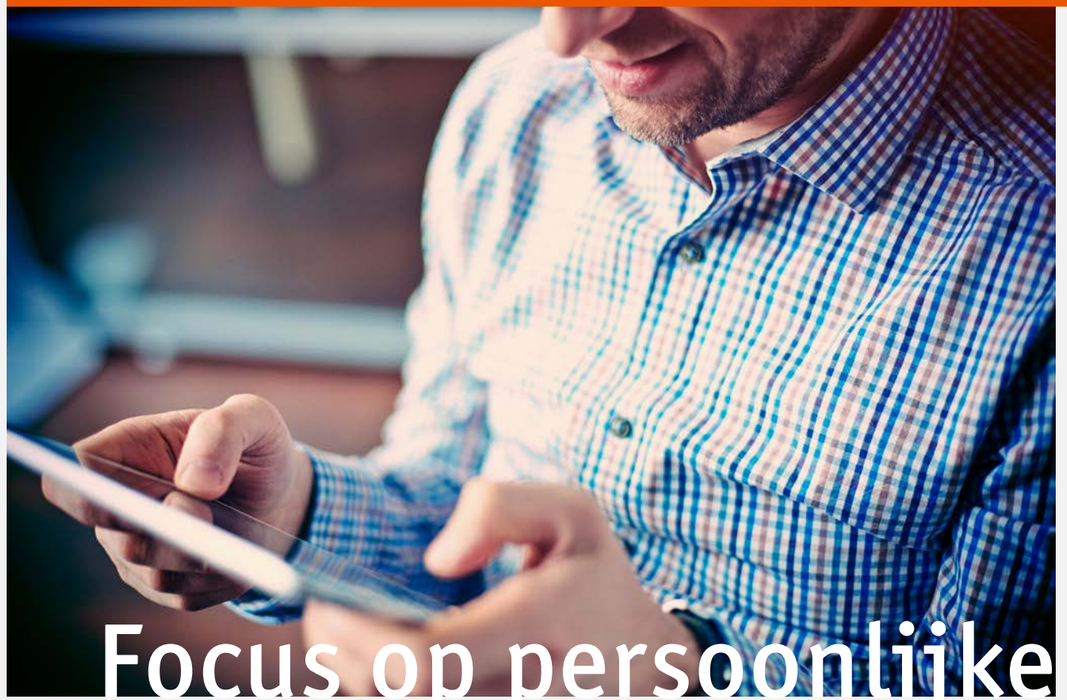
Veiligheid verzekerd

KPN verzorgt voor PROCURA de cloud-omgeving. Met PROCURA kwam het bedrijf met een bijzondere oplossing om gemeenten veilig en snel toegang te bieden tot het verkiezingspakket van PROCURA. Door PROCURA Verkiezingen vanuit CloudNL, de cloud-omgeving van KPN, op het Gemnet-netwerk aan te bieden, verwacht PROCURA dat maximale veiligheid én beschikbaarheid gegarandeerd is. Alleen gemeenten en andere lokale overheden zijn namelijk aangesloten op het Gemnet-netwerk dat bovendien volledig door KPN beheerd wordt. KPN garandeert PROCURA een beschikbaarheid van 99,9% voor data. Korten is overtuigd van de veiligheid van de oplossing. “Omdat KPN het Gemnet-netwerk volledig beheert en het een privaat, strak gereguleerd netwerk betreft, is de beveiliging optimaal. Met KPN hebben we bovendien goede afspraken over de beschikbaarheid gemaakt. Vooral tijdens de verkiezingsperiode. Zij zijn ervan doordrongen dat er vooral op de verkiezingsavond niets aan het toeval mag worden overgelaten. Daar doen ze dan ook hun uiterste best voor. Ik heb dan ook goede hoop dat de verkiezingen voor ons en onze klanten vlekkeloos verlopen.”

Gemnet-netwerk

Al meer dan vijftien jaar vinden gemeenten elkaar én andere overheden via het Gemnet-netwerk van KPN. Het netwerk verbindt mensen, objecten en instanties. Zo vormt het de basis voor de processen die plaatsvinden binnen de gemeenteorganisatie en daarbuiten. Alle overheden met een verbinding met het Gemnet-netwerk profiteren van een beheerde aansluiting met een landelijke dekking, breedbandige capaciteit, in een controleerbare, veilige omgeving. Met dat platform als basis, ontwikkelt KPN de voorzieningen die overheden nodig hebben. Denk daarbij aan toepassingen die in hun informatiebehoeftes tegemoet komen. Daarnaast kan het Gemnet-netwerk desgevraagd toegang verlenen aan applicaties van externe partijen en commerciële organisaties, waarvan lokale overheden vaak gebruik maken. Zoals bijvoorbeeld pakketten van PROCURA. KPN maakt in lijn met de wensen van gemeenten en andere lokale overheden afspraken met deze partners. Zo heeft de gemeente hier geen omkijken meer naar en kunnen partijen informatie veilig uitwisselen. Het Gemnet-netwerk biedt daarnaast toegang tot KPN-clouddiensten die extra gemak bieden, zoals Telefonie Online, Hosting, Beveiligde e-mail, mobiel werken, maar ook Data Hub Services voor onder andere Internet of Things-toepassingen. Met deze voorzieningen werken ambtenaren van een gemeente gemakkelijk en veilig samen.

Totaalleverancier voor verkiezingsmateriaal PROCURA levert sinds 1972 producten en diensten aan meer dan driehonderd gemeenten in Nederland. PROCURA is totaalleverancier van verkiezingsmateriaal (van stempassen tot stemhokjes), formulieren en drukwerk (van beveiligd papier tot trouwboekjes). Het bekendste PROCURA-product is de Gemeentelijke Basisadministratie persoonsgegevens (PROBEV). Een andere bekende dienst is de productie en levering van het papieren verkiezingsmateriaal. De verkiezingskalender en de materieellijsten zijn zo voor veel gemeentelijke ambtenaren belangrijke (controle)bronnen. Voor de productie en verspreiding werkt PROCURA samen met diverse grote drukkerijen door heel Nederland. PROCURA, gevestigd in Heerhugowaard, is onderdeel van de Conxillium Group B.V. Conxillium ontstond in 2015 bij het samengaan van de bedrijven BeheerVisie, GeoTax en JCC Software. Samen hebben ze als gemeenschappelijk doel: “Het verbeteren van de betrouwbaarheid van de lokale overheid.” Elke onderneming heeft binnen Conxillium zijn eigen applicaties en specialismen en werkt samen op basis van open standaarden en koppelingen.



Focus op persoonlijke en efficiënte dienstverlening

Digitale dienstverlening moet burgers en ondernemers zoveel mogelijk in staat stellen hun zaken zelf te regelen. Maar dat vraagt van overheden een geheel andere manier van denken en werken, eentje waarbij de termen persoonlijk en efficiënt centraal staan.

Met enige regelmaat hoor je burgers en ondernemers klagen over de dienstverlening van de overheid. Volgens hen moet en kan het allemaal efficiënter en met name persoonlijker. “Dat sluit goed aan bij onze visie”, aldus Herman Mansveld, senior business consultant bij Everest. “Wij geloven in het motto: digitaal waar het kan, persoonlijk waar het moet. In onze ogen betekent persoonlijk dat de klant/burger écht centraal staat en dat er gewerkt wordt vanuit zijn of haar mogelijkheden en behoeften. En daar waar burgers het te complex vinden om het digitaal zelf op te lossen, zouden zij moeten worden bijgestaan door deskundige ambtenaren. Die andere kijk op digitale dienstverlening vraagt om een proactieve overheid, waarbij gedacht wordt vanuit de kennis en de persoonlijke situatie van de burgers en ondernemers. Het vraagt óók om een overheid die transparant is en verantwoording aflegt over haar doen en laten. Dat betekent dat overheden anders moeten leren werken en denken.”

Wendbare technologie

Om overheden anders te leren denken en werken, worden door Everest technieken ingezet die modelgedreven en kennisgebaseerd zijn en die rekening houden met de dynamiek in regelgeving. Al die technieken komen samen in Blueriq, software voor Dynamic Case Management (DCM), waarmee de samenwerking tussen overheid, burger én bedrijven maximaal wordt ondersteund. Het brengt informatie, processen en mensen samen. Dat zorgt ervoor dat alle beschikbare en benodigde informatie actueel blijft en toegankelijk is voor alle betrokkenen. Door deze wendbare technologie worden de leefwereld van de overheid en die van de burger ‘aan elkaar geknoopt’, waarbij de termen persoonlijk en efficiënt centraal staan.

Mansveld spreekt tegen dat die termen tegenstrijdig zouden zijn. “Het beeld heerst dat maatwerk in relatie tot dienstverlening duur is”, zo schetst hij. “Maar dat is het juist niet. In de processen van de overheid zie je vaak dat (standaardisatie-) principes uit de maakindustrie zijn overgenomen. Tot op zekere hoogte werkt dat, behalve als je uit moet gaan van de persoonlijke situatie van de klant. Dat leidt ertoe dat iemand die niet in de standaardisatie past, uiteindelijk veel meer geld kost. Als een klant/burger niet in de standaard past, dan ontstaat er meer uitval, is er vaker sprake van het kastje en de muur, komen er vaker klachten en het uiteindelijke liedje is dat de ambtenaar meer moet improviseren om het alsnog voor elkaar te krijgen. Met andere woorden: maatwerk! Dan kun je beter meteen kiezen voor een oplossing à la Dynamic Case Management. Zet daar een vakman op die geen gedoe meer heeft met bijvoorbeeld het uitbesteden van activiteiten of het op orde krijgen van dossiers, waardoor hij zich alleen kan richten op de klant en op zijn vak. Dan ben je écht een stap verder. Dat is de lijn die wij hebben ingezet. Om onze klanten te ondersteunen in deze andere manier van werken en denken, is het opleidingstraject één van de pijlers.”

Blueriq Business Modeling Academy

De opleiding waar Herman Mansveld over rept, is de Blueriq Business Modeling Academy, een Everest-traject waarbij cursisten in acht weken worden klaargestoomd om succesvol te kunnen werken met het softwareproduct. Dat gebeurt in de vorm van trainingen, workshops en opdrachten. “Onze aanpak daarbij is uniek omdat wij niet denken vanuit bestaande processen”, zo zegt Menno Gülpers, opleidingsmanager Blueriq. “Wat je bij digitaliseringsstrajecten veel ziet is dat, op basis van bestaande processen, er nieuwe software wordt ingezet. Dat levert veelal geen meerwaarde op. Bovendien zet je dan de eigenaar van het systeem niet in zijn of haar kracht. Je wil graag dat de mensen die met het systeem werken, ook zingevend werk doen. Dit kan met de nieuwe mogelijkheden in IT, maar dan moeten we wel anders gaan werken en denken. De opleiding die wij bieden is dan ook meer dan het leren van een trucje. De cursisten leren hier een vak. Het leert hen op een andere manier ontwerpen. Een manier waarbij niet de IT centraal staat, maar juist de casemanager en dat wat hij nodig heeft om zijn werk goed te kunnen doen.”

Dit najaar heeft een groep van veertien cursisten met succes het eerste opleidingsprogramma rondom Blueriq afgerond. Daar blijft het niet bij, zo laat Menno Gülpers weten.

Het beeld heerst dat maatwerk duur is. Maar dat is het juist niet.

“In 2017 zetten we nog eens vier van dit soort opleidingsprogramma’s neer, waarmee wij cursisten afleveren die prima in staat zijn om burgers en ondernemers te ondersteunen als het gaat om persoonlijke en efficiënte dienstverlening. Zo zetten we een belangrijke stap om ons motto ‘digitaal waar het kan, persoonlijk waar het moet’ in de praktijk te brengen.”

Herman Mansveld,
senior business consultant
(h.mansveld@everest.nl)

Menno Gülpers,
opleidingsmanager Blueriq
(m.gulpers@everest.nl)

Winnaars van de VenJ Appathon

VenJ en politie halen de vernieuwing binnen

Een unicum in Nederland: het ministerie van VenJ nodigde externe partijen uit om in een Appathon mee te denken over een geluidsapp voor de politie. Bijna veertig app-ontwikkelaars doken in de wereld van veiligheid en gezag. Deskundigen vertelden over het belang van audio in het opsporingsproces.

Karina Meerman

Geluid speelt een belangrijke rol in de strafrechtketen, maar is niet eenvoudig vast te leggen op een manier die leidt tot betrouwbaar bewijs. Denk aan de politie die in de openbare ruimte verhalen van burgers hoort en moet noteren. Dat gebeurt vaak op plekken met veel omgevingsgeluiden, waar al dan niet meerdere mensen aanwezig zijn. Waar mensen ‘twee richtmicrofoons op hun hoofd’ hebben, de beschrijving van onze oren volgens geluidstechnicus bij de politie Dennis Bergfeld, nemen gewone microfoons ongefilterd alle geluid waar. Tikkende vingers op een tafel klinken dan, als de smartphone op tafel ligt en afhankelijk van de situatie, harder dan het stemgeluid. Daarbij is het technisch niet mogelijk om stemmen te scheiden. Wel is het mogelijk te filteren en ruis te verlagen. Bergfeld zou graag ruwe audio-data ontvangen van collega’s zodat hij in postproductie zoveel mogelijk bronmateriaal heeft om te bewerken.

Politieman Olof van der Ziel wil met een druk op de knop opnemen wat burgers op straat hem vertellen en dat koppelen aan de Mobiel Werken-app (zie kader) waar hij dagelijks mee werkt. Liefst met real-time vertaalfunctionaliteit. Wat men onderling zegt wordt misschien wel opgenomen, maar is niet altijd direct te verstaan. “Als het een taal is die ik niet spreek, hoe weet ik dan wat er nog meer speelt?”

Meldkamer en OM

En dan is er het operationeel centrum, voorheen de meldkamer, waar ieder jaar 2,6 miljoen gesprekken binnen komen. Daar zit veel emotie bij en onsamenhangende verhalen. Het kan onduidelijk zijn wie de beller is en waar deze zich bevindt. Toch moet al deze audio goed worden opgeslagen, zegt Frans Biegelaar van de eenheid Oost-Nederland. Omdat intonatie belangrijk is, omdat mensen gesprekken soms achteraf ontkennen, omdat collega’s iets willen terugluisteren. Vastleggen gebeurt overigens ook in woorden. Dat geldt ook voor alle verslagen en verhoren. Dat is een enorme hoeveelheid tikwerk. Hoeveel tijd zou een goede spraak-naar-tekst-functionaliteit kunnen besparen?

Aan het eind van de keten zit het Openbaar Ministerie (OM), een “belangrijke afnemer van processen-verbaal in welke vorm dan ook”, aldus Officier van Justitie Rick Mol. Het OM werkt al veertien jaar aan het ontwikkelen van een digitaal dossier. “Waar we vroeger al blij waren met een korrelige vlek op een beveiligingscamera moeten opnames nu betrouwbaar zijn en de authenticiteit gewaarborgd.”

Twee dagen denken

De ontwikkelteams die zich hadden aangemeld voor de ‘VenJ Appathon: van beeld naar geluid’ hadden de twee dagen in de Caballerofabriek in Den Haag echt wel nodig. De lijst met gewenste functionaliteit groeide met iedere spreker, maar niemand leek erdoor afgeschrikt. Twee dagen lang was de sfeer positief en het energieniveau hoog. Peter Muijen, vanuit het OM verbonden aan het programma ‘Digitaal Werken in de Strafrechtketen (DWS)’: “Met deze Appathon halen we de vernieuwing binnen. Die input uit de markt is onontbeerlijk.” Programmamanger DWS bij de politie Bas van Tol was verrast over de openheid van de spelers. “Team GlobalOrange vroeg of de app op termijn ook door burgers gebruikt mocht worden. Ik werd er stil van. Dat hadden de opsporingsorganisaties zelf nooit bedacht.” Paul Huijser van het programma Digi-OM: “Ze hadden die vraag ook voor zichzelf kunnen houden, maar door hem te delen, werd hij krachtiger. Dit is de manier om software-producten te maken. Nog te vaak ligt de nadruk op financiën, waardoor het vertrekpunt beheer is en niet de mensen die met de software moeten werken.” De drie waren het erover eens dat de technologie er is om de strafrechtketen digitaler te maken en betrouwbaar te houden. Ze hoopten aan de start van de Appathon dat de aanwezige denkkracht bestaande technologieën op een unieke manier zou combineren.

Winnaar ‘Verhoord’

Die hoop werd op zaterdag bewaarheid. Het beste functioneel ontwerp was van team Milvum, dat meedeed omdat “boeven niet vrijgesproken mogen worden op basis van slecht bewijs”, aldus teamlid Salim Hadri. Hun app ‘Verhoord’ verbetert het proces van verhoor tot en met de rechter, vond de jury. De app heeft onder andere een duidelijke aan-uitknop (de opname start zodra de app opent), een koppeling met de politie-app Mobiel Werken en een spraak-naar-tekst-functionaliteit. Inzet van blockchaintechnologie waarborgt authenticiteit en maakt de oplossing decentraal inzetbaar. De jury was zeer gecharmeerd van het zelflerende karakter van de app. Hoe meer informatie bekend is, hoe beter de app gaat werken. Het meest innovatieve idee kwam van team Anycode, vier jonge ondernemers die eerder dit jaar hun universitaire studie Informatica afrondden. Hun ‘Geluidsagent’ zet geluid om naar tekst in iedere taal om daarna vertaald te kunnen worden.

Bij de opening van de Appathon zei plaatsvervangend secretaris-generaal en CIO van VenJ Roland Barendse: “We zetten de luiken van het departement open om expertise van buiten naar binnen te halen.” Dat het zoveel moois zou opleveren, had niemand durven hopen.

Mobiel Werken App

De Basisomgeving Mobiel Werken is een politie-app waarmee agenten op hun telefoon de identiteit van mensen en paspoorten en rijbewijzen kunnen scannen. Ook kunnen er digitale boetes mee worden uitgeschreven en verwerkt. De app maakt daarbij gebruik van zowel interne als externe systemen om bijvoorbeeld te kijken of iemand gezocht wordt of gevaarlijk is. Ook openstaande boetes worden vermeld.

De politie wil de mogelijkheden van de app verder uitbreiden. Zo is het in Den Haag mogelijk om ter plekke aangifte te doen met de app en wordt de beschikbaarheid van de app verbreed naar andere afdelingen binnen het politiekorps, zoals de recherche.

Om te voorkomen dat via de mobieltjes gevoelige informatie op straat komt te liggen, zijn er extra veiligheidsmaatregelen genomen. Zo wordt er geen gevoelige informatie op het mobieltje bewaard. Raakt de agent de telefoon kwijt of wordt deze gestolen, dan is de inhoud van het toestel op afstand te wissen. Alle handelingen en informatie op de mobiele telefoon worden bovendien centraal opgeslagen en bewaard.

iBestuur mobility co-creatie

Het tweede iBestuur Mobility congres is een work-in-progress. Ruim twintig overheidsorganisaties – van gemeenten tot de Belastingdienst – markt, onderwijs en startups brengen in co-creatie tijdens besloten bijeenkomsten nog onontgonnen gebieden op het snijvlak van overheid en mobility in kaart. Van een overheidsbreed ontwikkelplatform tot security, van blockchain tot duurzaam mobiel en stressvrij 24/7 bereikbaar.

Op *20 april* presenteren de deelnemers de nieuwe ‘mobiele landkaart’ tijdens het iBestuur Mobility Congres 2017 in Den Haag. *Meer informatie: ibestuur.nl/mobility*

’ENSIA helpt bij verantwoording informatieveiligheid’

Medio 2017 gaan alle gemeenten werken met één zelfevaluatietool voor informatieveiligheid: ENSIA. “Dat vermindert de werkdruk en het helpt gemeenten om ‘in control’ te zijn”, stelt Franc Weerwind, burgemeester van Almere en voorzitter van de commissie Dienstverlening en Informatiebeleid VNG.

Door **Wilma van Hoeflaken**
Beeld **Lex Beers**

“In 2013 hebben gemeenten een VNG-resolutie aangenomen waarin staat dat informatieveiligheid een randvoorwaarde is voor de professionele gemeente. Daar moet het natuurlijk niet bij blijven”, zegt VNG-bestuurder Weerwind. “Gemeenten moeten hun informatieveiligheid effectief en efficiënt blijven inrichten en zorgen dat dit onderwerp hoog op de bestuurlijke en ambtelijke agenda staat.” Hij wijst erop dat niet de departementen de toezichthoudende rol vervullen, maar de gemeenteraad. In de resolutie hebben gemeenten afgesproken de gemeenteraad in het jaarverslag te informeren over informatieveiligheid. “Met ENSIA wordt het eenvoudiger hier invulling aan te geven. Dat versterkt de toezichthoudende rol van de raad ook op dit dossier.”

Auditlast verminderen

Met de resolutie namen gemeenten de BIG (Baseline Informatieveiligheid Nederlandse Gemeenten) aan als het gemeentelijke basisnormenkader voor informatieveiligheid. “Ze hebben zich gecommitteerd aan de implementatie van de BIG”, aldus Weerwind. “Daarnaast vroegen ze de minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) de audit- en monitorlast van gemeenten te verminderen. Dat gebeurt met het ENSIA-principe.”

ENSIA staat voor Eenduidige Normatiek Single Information Audit. De afzonderlijke audits en verantwoording voor de Basisregistratie Personen, de Paspoortenuitvoeringsregeling, DigiD, de Basisregistratie Adressen en Gebouwen, de Basisregistratie Grootschalige Topografie en Suwi (Werk en Inkomen) zijn opgenomen in één verantwoordingssystematiek die uitgaat van de BIG en aansluit bij de planning- en controlcyclus van gemeenten. De Informatiebeveiligingsdienst speelde een belangrijke rol bij de totstandkoming van de ENSIA-systematiek. Weerwind: “Het is een fantastisch samenspel van VNG, gemeenten en drie departementen, namelijk BZK, Sociale Zaken en Werkgelegenheid en Infrastructuur en Milieu.”

Bewustwording

ENSIA houdt in dat gemeenten één vragenlijst invullen voor een zelfevaluatie. De CISO of de functionaris informatieveiligheid is er verantwoordelijk voor dat de vragenlijst intern wordt uitgezet en tijdig wordt ingeleverd. De

Franc Weerwind, burgemeester van Almere en voorzitter van de commissie Dienstverlening en Informatiebeleid VNG: “Nu leggen gemeenten nog versnipperd verantwoording af en doen ze dingen dubbel. ENSIA zorgt ervoor dat het aantal vragen met 15 procent afneemt”.

Zaanstad: “Alleen maar voordelen”

Zaanstad is een van de pilotgemeenten. Wat zijn de ervaringen van CISO Linda Goedhart? “De vragenlijst is goed in te vullen als je enige voorkennis hebt van de BIG en van eerdere zelfevaluaties. Ik merkte wel dat collega’s die de vragenset voor het eerst zagen moeite hadden om de scope te bepalen. Ik heb samen met hen de vragenlijst ingevuld, zodat ik af en toe wat kon bijsturen. Het is een kwestie van wennen. De vragenlijst komt jaarlijks terug, dus het wordt vanzelf gemakkelijker.”

Wat levert het jullie op?

Goedhart: “Voorheen hadden we te maken met aparte normenkaders voor verschillende toepassingen. In ENSIA zijn de normenkaders op elkaar afgestemd. Je legt in één keer verantwoording af. Als je de vragenlijst hebt ingevuld heb je een goed beeld van de informatieveiligheid gemeentebreed, over afdelingen, systeemgrenzen en domeinen heen. Dit draagt bij aan de bewustwording over informatieveiligheid. Die is bij sommige beleidsvelden goed aanwezig en bij andere wat minder. Ik zie alleen maar voordelen.”

Tips voor andere gemeenten?

“Zorg voor een contactpersoon die het coördineert en die weet bij welke collega’s hij of zij moet zijn. De CISO (Chief Information Security Officer, nvdr) ligt voor de hand. Het kan handig zijn om voor alle betrokkenen een startbijeenkomst te organiseren. Zorg ook dat het gemeentebestuur geïnformeerd is, zodat de introductie straks geen verrassing is.”

zelfevaluatie is de basis voor verantwoording aan de raad en aan de toezichthouders. “Nu leggen gemeenten nog versnipperd verantwoording af en doen ze dingen dubbel. ENSIA zorgt ervoor dat het aantal vragen met 15 procent afneemt”, aldus Weerwind. “Het maakt het naar mijn mening doelmatiger en doeltreffender.”

Gemeenten ontvangen in juli 2017 de uitnodiging voor de zelfevaluatie. Zijn ze er klaar voor? “Het is een proces”, zegt Weerwind. “Er is nu een pilot bij zeven gemeenten. Functioneert het? Wat leren we ervan? KING heeft een impactanalyse uitgevoerd om te kijken of het goed werkt. Ik vind dit een wijze manier om deze systematiek in te voeren. Je begint klein en maakt het groter. Maar we moeten straks niet meteen hiep hiep hoera roepen. We moeten blijven kijken of het werkt en of we nog verbeterslagen kunnen maken.” Aansluiting bij de Informatiebeveiligingsdienst is hierbij ook belangrijk, vindt Weerwind. “Het maakt mij gelukkig dat alle gemeenten zijn aangesloten. Informatieveiligheid wordt steeds meer bestuurlijk gedragen. Dat bewustwordingsproces is het allerbelangrijkste.”

Bedrijfsvoering

Wat levert ENSIA gemeenten op? “Als ik puur kijk naar de verantwoordingssystematiek betekent het dat gemeenten de horizontale en verticale verantwoording over informatieveiligheid effectiever kunnen oppakken. De werkdruk vermindert”, zegt Weerwind. Maar belangrijker is dat het gemeente helpt ‘in control’ te zijn, vindt hij. “Het levert een gemeente op dat ze in haar bedrijfsvoeringsproces - waarin ze zo afhankelijk is van data – continuïteit en betrouwbaarheid garandeert op een steeds hoger niveau.” Hij stelt dat er veel op gemeenten af komt. “Het digitale landschap is in beweging. Als gemeente heb je overzicht nodig. Daar draagt ENSIA aan bij. Dat is niet alleen goed voor gemeenten, gemeenteraden en de departementen, maar ook voor onze inwoners. Daar werken we tenslotte voor.”

Den Bosch: “Zaken worden meetbaar gemaakt”

’s-Hertogenbosch is een van de pilotgemeenten. Wat zijn de ervaringen van CISO Arjan Kieboom?

“Voor ons was het allemaal redelijk bekend. Ons beveiligingsbeleid is al jaren gebaseerd op de code informatiebeveiliging en de BIG is daarop weer gebaseerd. ENSIA bouwt daarop voort. Dus voor ons is de impact niet zo groot.”

Hoe pakte hij het aan? “Ik heb het met het management besproken en met verantwoordelijken op andere afdelingen. Maar voor ons was het niet zo nieuw, eigenlijk is het een lopend proces.”

Wat levert het jullie op?

“ENSIA is de audit van de huidige werkwijze en in het verleden had je geen audits. Sommige zaken worden nu meer meetbaar gemaakt en andere zaken worden aangescherpt. Wat er verwacht wordt van een norm is bij ENSIA duidelijker dan wanneer je alleen naar de BIG kijkt. Dat biedt voordelen. Zo hebben we gezien dat we bij sommige normen de puntjes nog op de i moeten zetten. Dat gaan we dus doen.”

Tips voor andere gemeenten?

“De CISO is de aangewezen persoon om dit te coördineren. Die moet met belangrijke stakeholders de maatregelen bespreken waarvoor zij verantwoordelijk zijn.”

Het Bildt: “Nu gaan we gas geven”

Het Bildt is een van de pilotgemeenten. Wat zijn de ervaringen van Aart van Tuijl, verantwoordelijk voor informatiebeveiliging? “Eigenlijk moet een CISO ENSIA coördineren, daar hoort dit thuis. Ik ben geen CISO. Dat het bij ons anders gaat, heeft te maken met bijzondere omstandigheden. Per 1 januari 2018 maakt het Bildt deel uit van de nieuwe gemeente Waadhoeke.”

Hoe pakte hij het aan? “Wij zijn een kleine organisatie, dus de lijnen zijn kort. Ik kon snel schakelen met degenen die over expertise op de verschillende onderdelen beschikken. Ook sprak ik met onze samenwerkingspartners. We hebben een regionale sociale dienst Noardwest Fryslân en een Shared Servicecentrum Leeuwarden. Maar je blijft als gemeente natuurlijk zelf verantwoordelijk.”

Wat levert het jullie op?

“We zijn een nieuwe organisatie aan het bouwen en ENSIA staat hoog op de agenda, zowel bestuurlijk als ambtelijk. We zijn nog niet klaar met de implementatie van de BIG-maatregelen, maar ENSIA heeft ons een boost gegeven. Nu gaan we gas geven, met veel capaciteit, middelen, know-how en betrokkenheid.”

Tips voor andere gemeenten?

“Het is belangrijk dat het bestuur hier prioriteit aan geeft, dat het op de agenda komt en dat er tijd en geld voor gereserveerd wordt. Maak mensen enthousiast, zodat ENSIA breed landt in de organisatie. Ik zou de start markeren met een kickoff.”

Kijk voor meer informatie over ENSIA op www.kinggemeenten.nl

Frisse wind waait door gepokt en gemazeld bureau

Hennemann erkent dat PBLQ wat stoffig dreigde te worden. “Degelijk is goed en zegt ook iets over onze kwaliteit. Die kwaliteit is nog steeds onze kracht.” In de IASA (Interdepartementale Aanbesteding Strategische Adviesdiensten) van 2016 scoorde PBLQ in combinatie met het bureau Quint en onderaannemers TNO en ITSX het hoogste op kwaliteit. “Maar de ontwikkelingen in de markt vragen meer. Vroeger was in het land der blinden eenoog koning. Nu zijn er veel jonge hoogopgeleiden, die slim en creatief zijn. Die zijn ook nodig.” Hennemann is sinds 1 april algemeen directeur van het ruim 100 medewerkers tellende PBLQ, en leidt de takken Academie en Traineeship (jonge informatie professionals). Patty Heemskerk is directeur Advies. Twee directeuren zorgen voor meer draagvlak en maken minder kwetsbaar, menen ze.

Focus op de I

Hennemann heeft veel ervaring met IT in het publiek domein. Als ondernemer, manager en consultant. Hij begon zijn loopbaan als consultant bij IBM voor de gezondheidszorg. Daarna had hij een eigen data-informatiebedrijf in de sport en werkte hij als CEO bij Software Improvement Group (SIG). “Dit gezelschap kun je niet zomaar aansturen. Je moet het adviesvak kennen.”

Mede-directeur Heemskerk werkt daarentegen al vijftien jaar bij PBLQ. Ze combineert haar managementrol met het adviesvak. “Het is goed om met de poten in de modder te blijven staan. Bovendien is het leuk om inhoudelijk bezig te zijn.” Heemskerk was eerder management consultant bij Bakkenist en werkte bij een leverancier van zorginformatiesystemen. Ze delen beiden een medische achtergrond. Hennemann studeerde medicijnen en Heemskerk medische informatica.

Bij PBLQ, het adviesbureau voor de overheid, komt de focus nu nog meer te liggen op de I van informatiesamenleving. De nieuwe directeur Philip Hennemann wil de kwaliteiten van jong talent beter benutten: “Jongeren denken heel anders over de informatiesamenleving en geven ons daarmee nieuwe energie.”

De algemeen directeur looft het sterke netwerk van PBLQ en de hoeveelheid kennis en ervaring die er is. “Heel veel mensen hier zijn gepokt en gemazeld in het vak. Maar we konden de combinatie van onze drie takken beter benutten. Dat doen we nu veel beter.” Ook nam Hennemann afscheid van een aantal projecten. “We leggen de focus nu helemaal op de I van de informatiesamenleving. Alles wat de overheid levert heeft te maken met informatievoorziening. Die gaat straks nagenoeg helemaal digitaal.” Heemskerk legt uit: “Juist in die digitale transformatie kunnen wij een verschil maken omdat de impact van die verandering zo groot is. De transformatie stelt nieuwe eisen aan ambtenaren en overheden.”

Ook de opleidingskant van PBLQ past zich hierop aan. Hennemann: “Onze verbindersopleiding die vooral senior-mensen leert om beleid, uitvoering en IT in lijn met elkaar te brengen, bevat nu ook privacy-assessments, keteninformatisering en datamanagement. Allerlei onderwerpen die in de normale dagelijkse gang van zaken terugkomen. Geen verandering is nog zonder I.” Ook verzorgt het bureau maatwerkprogramma’s voor teams en organisaties in verandering.

Patty Heemskerk, directeur Advies, en Philip Hennemann, algemeen directeur, verhuizen met hun medewerkers naar de verbouwde locatie van PBLQ aan de Muzenstraat in Den Haag, vlakbij de meeste ministeries.

De Beeldredaktie

Volgens Heemskerk stond het traineeship voorheen meer op zichzelf. “Nu zoeken we veel meer de samenwerking. Een trainee werd altijd al begeleid door een adviseur, maar nu doen deze jonge informatieprofessionals ook mee met alle activiteiten die we voor de adviseurs organiseren. Hierdoor merken we een voortdurende kruisbestuiving van de jongeren en onze ervaren adviseurs. Qua kennis en nieuwe werkwijzen zoals Scrummen en Devops zijn jonge mensen sneller up to speed”, geeft ze aan. “Daarnaast zijn jongeren meer geneigd onbevangen naar vraagstukken te kijken en zien daardoor het burgerperspectief vaak beter. Ze stellen vaste patronen ter discussie en helpen ons te innoveren. Bijvoorbeeld doordat nieuwe onderwerpen aandacht krijgen zoals Blockchain.” Heemskerk zegt enorm te kunnen genieten van de samenwerking met de trainees.

Hennemann benadrukt dat het traineeship van het adviesbureau, anders is dan gemiddelde traineeships. “Onze jonge informatieprofessionals hebben al een aantal jaren werkervaring. Ze moeten een Master hebben en ze krijgen er nog een bij ons, namelijk in public information management.” Deze opleiding verzorgt PBLQ samen met de Erasmus Universiteit Rotterdam. Hoogleraren als Wolfgang Ebbers (innovatie en communicatie), Albert Meijer (publieke innovatie) en Victor Bekkers (Public Administration & Policy) nemen een deel van die opleiding voor hun rekening. Hennemann verklaart: “Je krijgt alleen de besten als je ook het programma aantrekkelijk maakt. Onze jonge informatieprofessionals zijn een maatje inhoudelijker en steviger dan andere trainees. We selecteren ze daarop. Vroeger was een trainee hier binnen twee jaar weg. Daarin zijn we flexibeler geworden.”

Afscheid van monument

En dan is er de samenvoeging van alle medewerkers op de geheel verbouwde locatie van PBLQ aan de Muzenstraat in Den Haag vlakbij de meeste ministeries. Hennemann: “Naast de Muzen bezaten we ook nog een prachtig oud pand aan de Van der Spiegelstraat. Maar echt praktisch was het niet, want iedereen zat verspreid over twee locaties en een deel van de ruimte gebruikten we niet. Met een lach en een traan hebben we afscheid genomen van het historische pand. Met als bijkomend voordeel dat we nu financiële ruimte hebben om te innoveren. Dit nieuwe pand markeert een nieuwe lente, een nieuw begin.” Heemskerk: “Het nieuwe pand past beter bij waar we nu staan. Bovendien zitten we nu dichter bij onze opdrachtgevers.”

PBLQ werkt aan grote programma’s die de digitale transformatie mogelijk maken zoals Operatie BRP en Idensys (eID). Hennemann: “Deze programma’s krijgen veel politieke aandacht en raken een veelvoud van partijen in de informatiesamenleving.” Ook de basisregistraties en de Omgevingswet zijn grote dossiers bij PBLQ, net als de veranderingen bij de Nationale Politie en de keteninformatisering in het veiligheidsdomein. Heemskerk: “De digitale overheid en met name de governance-vraagstukken, daar komen we traditioneel vandaan. We zijn goed in het beheersbaar maken van deze programma’s. We kijken methodisch hoe we processen kunnen verbeteren en bieden klanten daarmee houvast. Ook durven we zo nodig adviezen te geven die de opdrachtgever misschien niet leuk vindt om te horen, zoals het bijsturen of stopzetten van een project. Anders dan een IT-leverancier hoeven we onze IT-producten niet te slijten.”

Verbinding maken

Ze vervolgt: “Een opdrachtgever met een probleem help je niet altijd het beste met een advies, maar bijvoorbeeld ook met een opleiding of door naast een programmamanager een trainee te zetten. Bij advies blijf je afhankelijk van een derde, we willen de overheid zelf in haar kracht zetten. Ook omdat de intrinsieke motivatie voor een betere samenleving in onze genen zit. We zijn ooit door de overheid opgericht. Die wortels zitten in onze organisatie.”

Volgens Heemskerk zijn de consultants van concullega’s vaak vooral technisch georiënteerd. “Wij begrijpen IT en bestuur. Bedrijven worden ongeduldig als het beleid verandert, terwijl wij het juist interessant vinden. We zorgen dat de juiste partijen met elkaar praten zodat je toch verder kunt. We werken met alle stakeholders samen.”

De beide directeuren vinden het jammer dat er nog steeds veel aandacht is voor IT-projecten van de overheid die niet goed gaan. Heemskerk: “Grote IT-projecten zijn vaak negatief in het nieuws. Maar je kunt ook leren van projecten die goed gaan. We merken dat opdrachtgevers door deze negatieve aandacht eerder verlammen en meer regels bedenken.” Hennemann: “Dit is ergens begrijpelijk omdat de overheid in een glazen huis opereert met publiek geld. Maar juist voor veranderprogramma’s moet je lef hebben. De digitalisering is onvermijdelijk. Het is core business voor de overheid. Het is voor mij onbegrijpelijk dat er geen experimenteerruimte is. Dat is in elk bedrijf doodnormaal. En in elk project dat nieuw is gaan dingen mis. Dat hoort erbij en daar leer je van. De overheid zou daarin wat zakelijker mogen zijn. Daar helpen wij graag bij.”

Privacy en softwareontwikkeling

Het verwerken van persoonsgegevens is onderhevig aan wet- en regelgeving. Je mag gegevens niet gebruiken voor een ander doel dan waarvoor ze verzameld zijn. Je mag ze evenmin onnodig lang bewaren. Dus ook niet om software te testen of om problemen in bestaande toepassingen op te sporen.

Verleidelijk is dat wel. Het verwerken van persoonsgegevens gaat bijna altijd via software. Als je een nieuwe toepassing realistisch wilt testen, dan is het aantrekkelijk om echte persoonsgegevens te gebruiken. Hetzelfde gaat op voor probleemanalyses van operationele software.

Maar de Wet Bescherming Persoonsgegevens staat het gebruik van productiegegevens voor dit soort doeleinden meestal niet toe. Het is bovendien zeer onwenselijk dat personeel van de IT-afdeling toegang krijgt tot persoonlijke gegevens die niet voor hen bedoeld zijn. En afgezien van al het voorgaande: bedenk dat het merendeel van alle fraudegevallen van binnen uit komt. Bind dus niet de kat op het spek!

Hoe ontdek je het verschil tussen productiegegevens en random gegenereerde testdata? Dat is niet altijd even gemakkelijk. Stel dat productiegegevens door een zogenaamde ‘braatolizer’ (generator van nepgegevens, nvdr) zijn gehaald, dan kun je soms via een geospatiële analyse achterhalen of bestaande adresgegevens zijn gebruikt. Via algoritmes kun je vaststellen of postcodes bij plaatsnamen horen.

Via statistische tests valt soms vast te stellen of het om fake-data gaat. Maar ja, als die tests geen duidelijke uitslag geven, gaat het dan wel of niet om echte productiegegevens? Nazoeken met de hand is natuurlijk onbegonnen werk.

Er is nog een weg: de wet van Benford. Productiegegevens staan bol van het cijfermateriaal. In echte data komt het getal 1 als eerste cijfer het meest voor, en dat loopt af tot 9 met de minste kans. Dat is in 1937 beschreven door Frank Benford. De aanleiding was dat de eerste pagina’s van een logaritmisch tabellenboek veel beduimelder waren dan de laatste, dus meer bekeken. Hij onderzocht ook de eerste 342 adressen in de toenmalige American Men of Science en cijfers in Reader’s Digest. Zo ontwikkelde hij inzicht in patronen en uiteindelijk de zogeheten Benford-verdeling.

De uitkomst: als eerste cijfers in gegevensbestanden ongeveer Benford-verdeeld zijn, is de kans groot dat het om productiegegevens gaat. Met behulp van dit oude stukje wiskunde kun je vaak vaststellen of ontwikkelaars de beschikking hebben over privacy- of concurrentiegevoelige gegevens.

En als dat zo is? Ja, daar moet je dan als bestuurder wat mee.

Prof. dr. Chris Verhoef
Hoogleraar informatica en wetenschappelijk adviseur voor overheid en bedrijfsleven. Hij is bereikbaar via x@cs.vu.nl

Waarom een prijs?

iBestuur introduceert in 2017 een prijs voor goed opdrachtgeverschap. Waarom? Zonder goed professioneel opdrachtgeverschap lukt het niet complexe ICT-projecten tot een goed einde te brengen. Ook de commissie-Elias wees nadrukkelijk op het tekortschieten van professioneel opdrachtgeverschap als faalfactor. Grote projecten zijn complex en er is veel publiek geld mee gemoeid. Daarbij heeft men in de publieke sector te maken met politieke zijwind en ketens met ingewikkelde besluitvorming. Dat vereist grote stuurmanskunst van de opdrachtgever.

Wij willen met de prijs het belang van goed opdrachtgeverschap op een positieve manier benadrukken. Door goede opdrachtgevers in het zonnetje te zetten. En uit te leggen wat zij goed doen. Door een set criteria op te stellen beogen we ook de kwaliteit van goed opdrachtgeverschap een stap verder te brengen.

In juni 2017 reiken we voor de eerste maal de prijs uit. Naast de hoofdprijs komen er ook nog enkele prijzen in bepaalde categorieën.

We pakken dit serieus aan. Met een adviesraad die bestaat uit Maarten Hillenaar, Steven Luitjens, Nicole Stolk, Jaap Uijlenbroek en Arre Zuurmond. De uitvoering, die vanzelfsprekend geheel vertrouwelijk is, wordt in handen gelegd van PBLQ en de brancheverenging Nederland ICT.

Nieuw: iBestuur Prijs voor Goed Opdrachtgeverschap

It takes two to tango

Met de introductie van een nieuwe prijs voor goed opdrachtgeverschap wil iBestuur het belang daarvan op een positieve manier benadrukken. Door goede opdrachtgevers in het zonnetje te zetten. En uit te leggen wat zij goed doen.

Peter Lievense

Voor het welslagen van ICT-projecten zijn niet alleen deskundige, betrouwbare en fatsoenlijke leveranciers nodig, maar ook opdrachtgevers die aan dezelfde kwalificaties voldoen. De laatste jaren wordt in de publieke sector al nadrukkelijker gekeken naar de professionaliteit van het eigen opdrachtgeverschap. Maar er kan nog wel een tandje bij, dachten wij. En wij niet alleen. Daarom introduceert iBestuur in 2017 de Prijs voor Goed Opdrachtgeverschap.

Wij willen met de prijs goede opdrachtgevers in het zonnetje zetten. En uitleggen wat zij goed doen. Naast de hoofdprijs komen er ook nog enkele prijzen in bepaalde categorieën. De uitvoering is in handen gelegd van PBLQ, het adviesbureau voor de overheid, en de branchevereniging Nederland ICT.

Principes voor goed opdrachtgeverschap

Opdrachtgevers worden in vijf categorieën beoordeeld.

1. *Samenwerking, communicatie en organisatie*
   Hierbij gaat het onder andere om de effectiviteit waarmee de opdrachtgever de organisatie van en besluitvorming rond projecten bestuurt, de gehele duur ervan.
2. *Planmatige opdrachtverstrekking*
   Hierbij gaat het om die aspecten die een effectieve uitvoering van de opdracht mogelijk maken, zoals het formuleren van duidelijke acceptatiecriteria en het verantwoordelijkheid nemen voor contractuele afspraken.
3. *Capaciteit, deskundigheid en kwaliteit*
   Hierbij gaat het onder andere om het beschikbaar stellen van voldoende deskundig personeel, waardoor bijvoorbeeld optredende knelpunten professioneel kunnen worden opgelost.
4. *Kwaliteitsmanagement*
   Hierbij gaat het onder andere om goede systemen voor risicomanagement, (periodieke) audits en prestatiemeting.
5. *ICT-specifieke onderdelen*
   Hierbij gaat het onder andere om het beschikbaar hebben van een heldere referentie- en projectstart-architectuur.

Aanpak

De aanpak is de volgende. Allereerst hebben we een selectie gemaakt van een aantal grote publieke opdrachtgevers. Dat zijn er voor de eerste editie zo'n dertig. Vervolgens is geïnventariseerd welke leveranciers projecten hebben gedaan met meerdere van die opdrachtgevers. PBLQ ontwikkelt momenteel een vragenlijst en de ranking-methodiek in nauwe samenspraak met alle partijen.

Vervolgens wordt met deze vragenlijst een ronde gemaakt langs de geselecteerde ICT-leveranciers. Nederland ICT en PBLQ coördineren deze sessies, waarbij er wordt gesproken met een aantal vertegenwoordigers van elk bedrijf. Tot dusver zijn de twintig belangrijkste leveranciers daarvoor geselecteerd. Maar er komt ook nog een gecombineerde sessie met enkele kleinere gespecialiseerde leveranciers.

Vervolgens wordt op basis van alle scores de rangorde en de winnaar bepaald. Ook maken we de rest van de Top 5 bekend. Zij krijgen als daar voldoende aanleiding voor is ook een prijs, als ze excelleren op een specifiek aspect van de ranking. Vergelijk het met de Oscar-uitreiking: beste regie, beste acteur... enzovoort.

De ranglijst op zich blijft vertrouwelijk. Maar opdrachtgevers die nieuwsgierig zijn naar hun prestaties, kunnen wel inzicht krijgen in hun eigen positie en scores, maar wel uitsluitend in de waardering van hun eigen organisatie.

De uitreiking is naar verwachting medio juni.

Gevoelig

Wij begrijpen dat het opstellen van ranglijsten een gevoelig onderwerp is. Niet alleen voor de beoordeelde opdrachtgevers, maar ook voor de beoordelende leveranciers. Het is niet onze bedoeling met dit initiatief aan *naming and shaming* te gaan doen. Integendeel, het gaat ons er juist om het belang van goed opdrachtgeverschap te benadrukken. En om duidelijk te maken wat goede opdrachtgevers goed doen en wat goed opdrachtgeverschap inhoudt. Dat nu overheid én bedrijfsleven gezamenlijk een set kenmerken opstellen die goed opdrachtgeverschap definiëren, lijkt ons sowieso al pure winst. Daar kan iedereen zijn voordeel mee doen. De selectie en de methodiek zullen deze eerste editie mogelijk nog kinderziekten vertonen, maar we pakken het zo zorgvuldig mogelijk aan. We gaan het gewoon doen. Het hogere doel van alle betrokkenen is het verbeteren van de publieke sector – en in dit geval het opdrachtgeverschap.

Samenwerken beperkt schade

Voorkomen kun je een datalek niet, maar preventieve maatregelen nemen en weten wat je moet doen kan de schade flink beperken. VenJ en Logius sloegen de handen ineen om gezamenlijk informatie over datalekken te versterken.

Door **Marie Louise Borsje**
Beeld **Dreamstime**

Het onderwerp datalekken is erg actueel. Sinds 1 januari 2016 geldt de meldplicht voor datalekken. Een fikse boete van de Autoriteit Persoonsgegevens hangt je boven het hoofd als een datalek in een systeem waar je verantwoordelijk voor bent, niet tijdig wordt gemeld. Zo heeft KPN pas een flinke boete gekregen doordat zij niet juist gehandeld hadden na het constateren van een datalek.

Henk-Jan van der Molen, Corporate Information Security Officer (CISO) bij VenJ: “We spreken van een datalek als iemand zich onbevoegd toegang verschaft tot persoonsgegevens. Het doet er niet toe of die persoon dan wel of geen wijzigingen aanbrengt in de data. Het gaat hierbij dus specifiek om persoonsgegevens. Als iemand toegang krijgt tot andere informatie, dan noemen we dat een informatielek.”

“Als het alleen NAW-gegevens zijn, is er weinig risico”, vervolgt Roeland Derksen (Logius), “Het is de combinatie van gegevens die een gevaar kan zijn of zelfs heel pijnlijk.” Snel worden de mobieltjes gecheckt om een beruchte hack op te zoeken. “De Ashley Madison-hack (2015) is zo’n voorbeeld van een pijnlijk datalek. Dat is een datingsite voor mensen die al een relatie hebben. Je kunt je voorstellen dat het lekken van persoonsgegevens een enorme impact kan hebben op iemands leven. We zijn erg alert op datalekken met combinaties die met overheidsgegevens te maken hebben. Denk aan DigiD waar Logius verantwoordelijk voor is en aan strafrechtelijke gegevens van het ministerie van Veiligheid en Justitie.”

Maanden

Het kan een hele tijd duren voordat je doorhebt dat er een datalek is. “Soms lift een besmet bestand mee met een ander bestand en kan het een paar maanden duren voordat het lek zich manifesteert. Je merkt het vaak aan reacties uit je omgeving: ‘Ik krijg vreemde berichten van je’ of ‘Jouw systeem doet raar’. Wat je dan moet doen is in ieder geval zo snel mogelijk aan de slag om het lek te dichten en tegelijkertijd denk je na over de vervolgstappen. Welke data zijn blootgesteld? Welke risico’s zijn er? Wie moet je informeren en hoe? Hieraan zie je ook meteen dat het verstandig is om van tevoren na te denken over datalekken en als het kan ook om te oefenen met een crisisorganisatie. Bij datalekken ligt de aandacht vooral op het voorkomen ervan door preventieve maatregelen. Het is net zoals bij inbraak: als een dief veel tijd heeft en koste wat kost naar binnen wil, dan lukt dat vaak ook. Je kunt natuurlijk wel maatregelen nemen om het hackers lastig te maken of om de risico’s zo klein mogelijk te houden.”

Sandra van Denderen werkt als crisiscommunicatiespecialist bij Logius. “We hebben afgelopen week nog geoefend met een crisissituatie. Dat is erg belangrijk. Zo weet je precies wie wanneer wat moet doen. We zorgen voor up-to-date draaiboeken voor crises en organiseren opleidingen. Verder ontwikkelen we scenario’s: wat zou er eventueel kunnen gebeuren? En wat zijn de risico’s daarvan? Hoe moet je handelen?” Dan gaat haar telefoon: ze heeft piketdienst en er is een incident. Roeland gaat verder: “Het correct melden van een incident is wel een punt van aandacht. Als je een melding van een lek maakt terwijl er niets aan de hand is kan dat ernstige imagoschade opleveren voor een overheidsorganisatie. Mensen denken dan: ‘wat is dat voor een zooitje daar?’ We kunnen het niet vaak genoeg zeggen: de enige manier om goed met datalekken om te kunnen gaan is door goede voorbereiding. Oefen met een crisisorganisatie, maak scenario’s en zorg dat je kennis up-to-date is!”

Handreiking

Logius en VenJ zijn hiermee aan de slag gegaan en hebben samen een handreiking en een factsheet ontwikkeld. Henk-Jan: “Hoewel deze documenten zijn gemaakt voor VenJ kunnen ze met wat copy-paste ook door andere organisaties worden gebruikt. In de handreiking staan verschillende mogelijke scenario’s en de manier waarop je die moet tackelen. In de factsheet staat de belangrijkste informatie over datalekken en de meldplicht op een rij. Geoefend met een crisisorganisatie voor datalekken hebben we bij VenJ nog niet, maar alle directies zijn wel geïnformeerd.”

“De documenten en kennis van VenJ in combinatie met de kennis van Logius geeft een mooie basis ook andere overheidsorganisaties te informeren. We vinden het belangrijk om onze kennis en ervaringen te delen. Daarom hebben we ook met z’n vieren een workshop gegeven tijdens de Ambtenaar 2.0 Dag. Daar merkten we dat er veel behoefte is aan informatie”, zegt Monique Barnhoorn die eerder werkte bij het ministerie van BZK en nu bij VenJ. Zij zorgde voor de verbinding tussen Logius en VenJ. “We leren zelf ook steeds bij en zoeken ook contact met andere overheden. Behalve bij Logius en bij VenJ kunnen ambtenaren ook terecht bij KING en NVVB voor kennisdelen en informatie.”

Handreiking datalekken:
http://bit.ly/handreikingdatalekken
Factsheet datalekken:
http://bit.ly/factsheetdatalekken

Doorstaat uw organisatie de privacy-proef?

Julian Vermolen (l) en Gerard Stroeve (r)

In het internettijdperk vervaagt de scheidslijn tussen privé en openbaar. Maar niet alleen vrienden en familie volgen ons makkelijker dan ooit. Weet u waar uw persoonsgegevens allemaal bewaard worden? Gerard Stroeve en Julian Vermolen, security & privacy-specialisten bij Centric, gaan in op de ontwikkelingen op het gebied van privacy en dataprotectie.

Waarom is privacy juist nu zo'n belangrijk onderwerp?

Gerard: "Vooropgesteld: privacy is altijd al een belangrijk goed geweest en ons recht erop is vastgelegd in de grondwet. Maar inderdaad, de laatste jaren krijgt met name de informationele privacy meer aandacht. Dat hangt direct samen met de technologische ontwikkelingen van de laatste jaren en het steeds belangrijker worden van digitale informatie in ons dagelijks leven. Het wordt steeds moeilijker om grip te houden op de digitale gegevens die van en over ons worden verwerkt."

Julian: "Eenmaal op het internet is het vrijwel onmogelijk om te achterhalen waar gegevens allemaal zijn opgeslagen. Bovendien worden gegevensverzamelingen vaker 'aan elkaar geknoopt' om functionele of commerciële voordelen te behalen. En natuurlijk vraagt ook de populariteit van sociale media als Facebook aandacht voor privacy. De huidige wetgeving kan de vraagstukken die hieruit volgen niet goed beantwoorden. Daarom zijn er passende en eenduidige nieuwe regels nodig."

Welke nieuwe regels zijn er?

Gerard: "Zowel binnen Nederland als op Europees niveau is er aan nieuwe wetgeving gewerkt. Sinds 1 januari 2016 is in Nederland de meldplicht datalekken van kracht, als onderdeel van de Wet bescherming persoonsgegevens. Daarnaast geldt vanaf 25 mei 2018 de zogenaamde Algemene Verordening Gegevensbescherming. Deze Europese verordening zal zonder nationale omzetting rechtsreeks en onverkort van toepassing zijn in alle Europese lidstaten."

Wat gaat de Europese wetgeving betekenen?

Gerard: "Deze verordening gaat op veel punten verder dan de huidige Nederlandse regels. Zo vraagt zij structurele, specifieke aandacht voor privacy binnen processen waarin persoonsgegevens worden verwerkt. Privacy wordt nadrukkelijk niet meer facultatief. Daarnaast komen er forse sancties voor het niet op orde hebben van de privacy."

Wat voor stappen kunnen organisaties zetten?

Julian: "Centric ondersteunt organisaties bij de voorbereiding op de nieuwe Europese wetgeving. Op bestuurlijk of strategisch niveau kun je bijvoorbeeld alvast een visie en een strategie formuleren. Denk na over hoe je de aandacht voor privacy borgt en het proces rondom gegevensbescherming inricht. Wie wordt verantwoordelijk voor de coördinatie van de diverse activiteiten op dit vlak?"

Gerard: "Verder is het een goed om alvast een beeld te hebben van de verwerkende processen en welke persoonsgegevens daarin gebruikt worden. Daarna volgt: in hoeverre voldoen deze processen al aan de diverse componenten van de aanstaande wetgeving? Kortom: hoe goed voldoet u op dit moment al aan de regels van de nabije toekomst? Het tijdig treffen van voorbereidingen helpt namelijk om de nieuwe wetgeving soepel te implementeren. Zo doorstaat uw organisatie uiteindelijk de 'privacy-proef'."

Tien hoofdpunten van de Algemene Verordening Gegevensbescherming

Beleid, visie en strategie
Organisaties moeten bewust aandacht geven aan passende bescherming van persoonsgegevens. Dit vereist een heldere visie, een gedegen strategie en de inrichting van een privacy-proces.

Beginselen inzake verwerking persoonsgegevens
Het verwerken van persoonsgegevens moet aan een aantal beginselen voldoen. Zo moet de betreffende verwerking rechtmatig, behoorlijk en transparant zijn. Ook moeten de persoonsgegevens toereikend, juist, actueel, ter zake dienend en beperkt tot het noodzakelijke, zijn.

Functionaris Gegevensbeheer
Organisaties die (gevoelige) persoonsgegevens verwerken en overheidsinstanties, moeten een functionaris voor gegevensbescherming aanstellen.

Gegevensbeschermingseffectbeoordeling
Voor bepaalde verwerkingen moet de organisatie een beoordeling uitvoeren van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens.

Passende informatiebeveiligingsmaatregelen
Organisaties moeten de persoonsgegevens beschermen met passende technische en organisatorische beveiligingsmaatregelen. Dit betekent dat de maatregelen volgen uit een risicoanalyse, aansluiten bij de standaarden in de markt en worden geïmplementeerd conform de opvatting 'data protection by default and design'.

Transparantie en toestemming
Organisaties moeten hun privacy-beleid in heldere, begrijpelijke taal inzichtelijk maken. Bovendien is expliciete toestemming van de betrokkenen vereist voor het verwerken van persoonsgegevens.

Recht op informatie en inzage
Betrokkenen hebben het recht om informatie te ontvangen over welke persoonsgegevens, op welke wijze en met welk doel worden verwerkt en welke functionarissen deze gegevens kunnen inzien.

Recht op rectificatie, wissing en overdraagbaarheid
Organisaties zijn verplicht persoonsgegevens aan te passen en/of volledig te wissen als de betreffende persoon daar om vraagt.

Meldplicht datalekken
Een inbreuk in verband met persoonsgegevens moet zonder onnodige vertraging en zo mogelijk binnen 72 uur aan de toezichthoudende autoriteit gemeld worden.

Versterking sancties en toezicht
Organisaties die zich niet aan de regels houden, riskeren boetes oplopend tot 20 miljoen euro of 4 procent van de wereldwijde omzet, indien dit cijfer hoger is.

Beeld: Dreamstime

Privacy: ‘From No to Know’

Aandacht voor privacy is begrijpelijk en nodig. Het is een tijdperk van meer regels en meer dreigingen. En ook van meer potentiële kosten, in reputatieschade en op te leggen sancties. Gelijktijdig neemt het privacy-bewustzijn bij burger en consument toe. Hoe kunnen we de privacy beschermen zonder de innovatie te remmen? Schets van een aantal ontwikkelingen.

De zogenaamde ‘Digital Convergence’, waarin de ontwikkelingen rond Big Data, het Internet of Things, Analytics, Cognitieve Systemen en Cloud bij elkaar komen, lijkt soms als één grote golf op ons af te komen. Wordt privacy in die ontwikkeling een belemmerende factor (NO) of is daar, uiteraard op een verstandige manier, een mouw aan te passen? (KNOW).

KNOW: De mogelijkheid om productiviteitsstijgingen en kostenbesparingen te realiseren door met zoveel mogelijk en zo toepasbaar mogelijke data aan de slag te gaan.

NO: Beperkingen die privacy-regels of –zorgen opwerpen. Zoals het ontbreken van transparantie en controleerbaarheid, onduidelijkheid waar ‘mijn’ data is opgeslagen en hoe er mee wordt omgegaan. Ook met het eventuele verplaatsen van data: welke locaties, welke landen zijn geschikt?

Be prepared

Het wordt tijd om een brug te slaan tussen de wereld van de wet- en regelgeving en die van de technologie. Be prepared! De befaamde basketbal-coach John Wooden zei ooit: “Als je al geen tijd hebt om het de eerste keer (goed) te doen, wanneer heb je dan de tijd om het óver te doen?”
Vaak worden privacy- en beveiligingswaarborgen áchteraf toegevoegd, als de noodzaak daartoe op vervelende wijze is gebleken. Dat leidt tot hogere kosten en grote implementatie-complexiteiten. Hoeveel verstandiger is het niet om van te voren stil te staan bij te nemen maatregelen? Privacy en Security moet een vanzelfsprekendheid zijn, en in het DNA van een organisatie aanwezig zijn. Privacy by Design dus.

Onderdeel van een tijdige aanpak is een programma voor de beveiliging van kritieke data en daarbinnen van de echte ‘kroonjuwelen. Beoordeel de eigen securityprocessen en/of -controles en maak een gap-analyse. Werk met hypotheses. Op bestuurlijk niveau heeft onder ander de Taskforce BID (Bestuur en Informatieveiligheid Dienstverlening) daar op behartenswaardige wijze aandacht voor gevraagd.

Een belangrijk uitgangpunt is om maatregelen ‘fit-for-purpose’ toe te passen. Waar data gebruikt wordt voor initiële of verkennende doelstellingen past een ander en soepeler beleid dan wanneer data gebruikt wordt voor het ondersteunen van bedrijfskritische beslissingen.

Digitale waakhond

IBM Research werkt aan het concept van de ‘Digital Guardian’, met als doel de kernvraag te kunnen beantwoorden: bent u ‘U’ wel? Door slimme analysetools te gebruiken kunnen we waarnemen of en hoe er contact wordt gemaakt met bedrijfsmiddelen en bouwen we een risicoprofiel op voor elk van deze bedrijfsmiddelen. Data mining-technieken, machine learning en cognitive computing worden gebruikt om modellen te bouwen, normale gedragingen vast te leggen en afwijkende activiteiten te signaleren. We noemen dat Security 360. Het geheel wordt vervolmaakt met een scala van security-controls die elk moment op risico’s kunnen anticiperen. Zo verraadt de misbruiker van de verloren smartphone zich bijvoorbeeld door zijn afwijkende manier van bedienen. En zo kan een lage afrekening bij een tankstation de alarmbel doen rinkelen omdat de digitale waakhond weet dat uw tank nog bijna vol is, en dat u nooit tankt als uw tank nog meer dan een kwart gevuld is. Daarbij: u bent toch op kantoor terwijl de transactie wordt geregistreerd?

Lerende systemen

Dergelijke lerende systemen kennen u, helpen u en beschermen u. Ze worden bovendien steeds doeltreffender omdat we steeds meer van ons leven digitaal documenteren. Een eerste generatie van dergelijke systemen noemen we ‘Cognitive Security’: beveiligingssystemen die herkennen, redeneren en leren van dreigingen. Eigenlijk hebben we het over het inbouwen van beveiligingsinstincten en – expertise. Die expertise wordt gevoed door geautomatiseerde analyse van onderzoeksrapporten, webteksten, dreigingsdata en andere relevante gestructureerde en vooral ongestructureerde data. Precies zoals cybersecurity-analisten elke dag doen, maar dan op een nog nimmer vertoonde schaal. En al deze opgedane kennis kan weer worden gedeeld met de menselijke analisten. Dat is de kern van Cognitive Security.

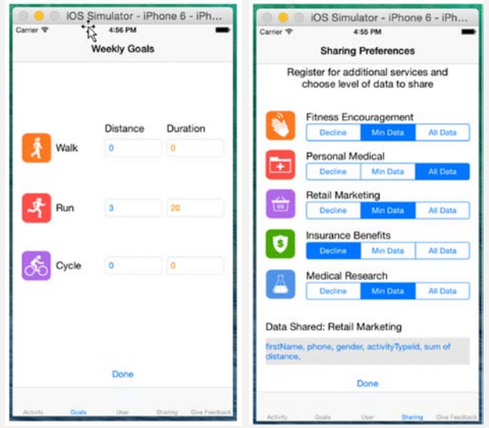
Privacy Based Access Control

Een laatste ontwikkeling waarin voortgang wordt geboekt: Privacy Based Access Control. Wie leest de gebruikersvoorwaarden van die nieuwe app? Bijna niemand natuurlijk. We drukken op de AKKOORD-knop om snel verder te kunnen. Dat moet dus anders, zeker als het om contact tussen burger en overheid gaat of om zaken doen: privacy based consent management.

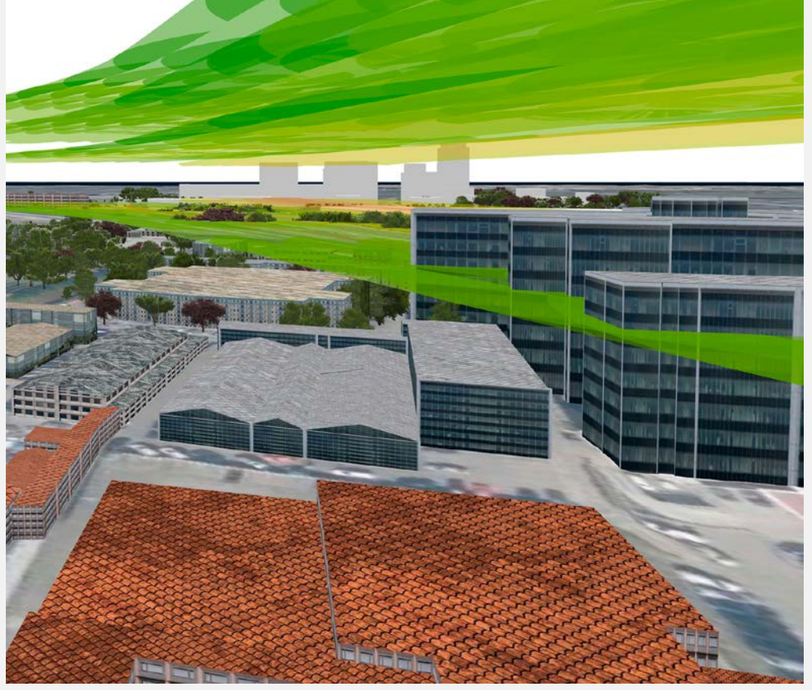
Daarbij leg je als gebruiker vast welk niveau van informatie je wilt delen met wie, mét inzicht in de data-elementen die gedeeld worden. Geen lange en ingewikkelde privacy statements meer de niemand begrijpt. De gebruiker beheert zelf tot op welk niveau de app data verzamelt deelt door op eenvoudige wijze de eigen voorkeuren vast te leggen. Dat werkt op basis van tevoren geformuleerde gebruiksregels (‘policies’). Zie als voorbeeld bijgaande fitness app. Een zeer wenkend perspectief!

Erno Doorenspleet, Executive Security Advisor en Rob Nijman, Client Relationship Executive Central Government, IBM Nederland B.V.

Fitness app: Privacy-Based Consent Management



Dynamisch 3D-stadsmodel helpt bij Omgevingswet en stadsbeheer



3D of 2D? Geluidsintensiteit in de Binckhorst. Links: na projectontwikkeling, rechts: huidige staat.

Gemeente Den Haag wil met 3D-kaarten werken

De gevolgen van ingrepen in de leefomgeving zijn veel eenvoudiger te tonen en door te rekenen met een driedimensionaal basismodel van de stad. Met de Omgevingswet in aantocht wordt dat gemak nog belangrijker. Den Haag experimenteert ermee.

Neemt dat ene geplande kantoorgebouw niet te veel zonlicht weg bij de buren? En krijgen de gebruikers niet bovenmatig last van verkeersgeluid? Wat zijn de leefbaarheidseffecten als het kantoor op die plek wordt neergezet? Het zijn voorbeelden van vragen die keer op keer moeten worden onderzocht bij ingrepen in de leefomgeving. De Omgevingswet, die over enkele jaren van kracht wordt, verenigt tientallen wetten waarin die aspecten zijn geregeld. Hoe mooi zou het dan zijn als dat soort zaken door een planontwikkelaar integraal zijn door te rekenen en te visualiseren?

Om te kijken of dat daadwerkelijk mogelijk is, is de gemeente Den Haag het project 'Dynamisch 3D-model' gestart. "Het kernidee is het gebruik van geo-informatie om de onderwerpen van de Omgevingswet – zoals geluid, lucht, bodem en water – inzichtelijk te maken. Door een geïntegreerd systeem te creëren, waarin rekenmodellen en informatiebronnen samenkomen, is een antwoord te geven op de ruimtelijke vragen die voortkomen uit die wet", zegt Jeroen Schilleman, adviseur geo-informatie voor de gemeente Den Haag.

Onderzoekskosten

Het is nog even wachten op de Omgevingswet en het is nog niet helemaal duidelijk hoe de vele informatiestromen in het Digitaal Stelsel Omgevingswet zullen lopen, maar dat is voor de gemeente Den Haag in dit geval geen reden om af te wachten, zegt hij. "Als we maar weten welke data we kunnen gebruiken." Het project is vooral opgezet om van te leren en om aan te tonen dat er al heel veel kan. En de belangrijkste reden om die weg in te slaan is dat op die manier de onderzoekskosten omlaag kunnen.

Schilleman legt het uit: "Voor een geluidsstudie bijvoorbeeld wordt nu een complete 3D-omgeving gebouwd. En dan worden er voor het onderzoeksgebied mensen het veld in gestuurd om metingen te doen, dat wordt vervolgens in een GIS-systeem – in het geval van de Gemeente Den Haag inArcGIS – geladen om daar vervolgens berekeningen op los te laten, met een rapport als resultaat. Als dat soort data al integraal voor de hele stad voorhanden zijn, zullen dat soort individuele onderzoeken niet meer nodig zijn." Nu wordt de verzamelde informatie na zo'n geluidsstudie vaak weer weggegooid. "Maar wij kunnen hetzelfde gebouwmodel gebruiken om te visualiseren wat er gebeurt als er brand uitbreekt." Ook voor onderzoek naar luchtverontreiniging of de bezonning van gebouwen is zo'n model dan inzetbaar. En met een 3D-visualisatie van de situatie gaat het overleggen voor burger/bedrijf (vergunningaanvrager) en ambtenaar (vergunningverlener) natuurlijk een stuk makkelijker.

Sleutelen

De ideale brondata om een 3D-model op te baseren is doorgaans die in de BAG, de Basisregistraties Adressen en Gebouwen. Deze tweedimensionele gegevens zijn betrouwbaar Voor de hoogtegegevens – bijvoorbeeld nodig om de bezonningsgraad van verschillende verdiepingen in een gebouw vast te stellen – wordt vervolgens gekeken naar andere referentiebestanden, bijvoorbeeld eigen luchtfoto's of het Algemeen Hoogtebestand Nederland. Maar bij panden met een complexere vorm bieden die gegevens nu nog onvoldoende houvast.

Momenteel doet Den Haag pilotprojecten op specifieke thema's. "Dat zijn niet alleen onderwerpen als geluid of lucht, maar ook samenwerkingsverbanden of specifieke ingrepen in de ruimte. Dan wordt er gekeken of deze manier van werken meerwaarde heeft. Het heeft tijd nodig." Zo moet het bijvoorbeeld eenvoudig worden om BIM-modellen (die in de architectenwereld gebruikelijk zijn) in één keer in het 3D-model te plaatsen. Ook verkeersinformatie zou in het model moeten passen, evenals een bestand met alle bomen in de gemeente. Data-integratie is dus belangrijk en daarbij helpt de software van Esri die Den Haag gebruikt. "Het spreekt voor zich dat het allemaal met elkaar moet kunnen praten en technisch kan het ook vaak, maar organisatorisch is dat best een uitdaging. Daar ben ik behoorlijk mee bezig in Den Haag." Ook overleg met andere partijen over de aanpak en standaardisatie blijft daarbij belangrijk.

Schillemans afdeling zoekt bijvoorbeeld de samenwerking met het Kadaster, maar ook met de gemeente Rotterdam en de gemeente Westland. "In het Westland heb je door de hoeveelheid kassen een heel andere situatie in het model. Van hun ervaringen leren we graag; we zoeken samenwerkingen actief op."

Januari

17 januari — ICTU Café
Innovatie in de binnenvaart, met RWS
ICTU, Den Haag
www.ictu.nl

22 januari — eHealth Steden Estafette
HagaZiekenhuis, Den Haag
http://bit.ly/2hsPcdy

Februari

2 februari — Op digitale expeditie; 10 jaar Forum Standaardisatie
Malietoren, Den Haag
http://bit.ly/2i73Hof

7 februari — iBestuur symposium in Nieuwspoort
Grip op privacy
Nieuwspoort, Den Haag
zie pagina 39 in dit magazine

Maart

22 maart — VNG Ambtelijke Top conferentie:
Samenwerken in de informatiesamenleving
locatie nog te bepalen
http://bit.ly/2hwbHzY

April

5 april — KING: Congres Digitale Agenda 2020
de Fabrique, Maarssen
http://bit.ly/2iDURLE

iBestuur magazine, januari 2017
iBestuur magazine is een onafhankelijke uitgave van de Nieuw Domein Uitgever.
Uitgever Peter Lievense
Redactieadres
iBestuur magazine
Jan van Nassaustraat 57
2596 BP, Den Haag
redactie@ibestuur.nl
Hoofdredactie Peter Lievense
Ontwerp en vormgeving Blinkerd
Eindredactie Freek Blankena

Medewerkers Frits de Jong, Bas Linders, Karina Meerman, Fred van der Molen, Peter Mom, Peter Olsthoorn, Petra Pronk, Nicole van der Steen, Fred Teunissen, Marieke Vos, Brenno de Winter, Marijke van Hees, Peter van Schelven, Sophie in ‘t Veld, Chris Verhoef, Marie Louise Borsje.

iBestuur.nl Kees Brandenburg, met dank aan textpattern
Fotografie en illustratie De Beeldredaktie, Lex Beers, Marijn van Bekkum, Blinkerd Dreamstime, Shutterstock, Stockfresh
Cover voor Lex Draijer/De Beeldredaktie
Cover achter Blinkerd
Proces en realisatie Bos Uitgevers
Druk BDU
Advertenties advertenties@ibestuur.nl

Een iBestuur magazine-abonnement is gratis voor bestuurders, beslissers en beleidsmakers binnen de publieke sector die betrokken zijn of zich betrokken voelen bij de i-overheid.
Geïnteresseerden die niet tot die doelgroep behoren betalen 70 euro voor een jaarabonnement van vier nummers. Abonneren kan via ibestuur.nl/service.

iBestuur wordt mede mogelijk gemaakt door:
Capgemini, Centric, CGI, Everest, IBM, Imagem, KPN, PinkRoccade Local Government, en door ICTU, KING en PBLQ.


DE TIJD
'Hoe is het met jij?'
HANDELSREIZIGER IN TAAL Wim Daniels
15 MAART 2017
Als Wilders wint?
Chantal Mouffe over links populisme
ELSEVIER
iBestuur
magazine
Anoniem
Juist
ELSEVIER
Vrij
Op de brommer door Uruzgan
Jeroen Brouwers over het raadsel Joost Zwagerman
Wilders
Zo gaat links