

Hét platform voor de informatieprofessional bij de overheid

SECURITY EN PRIVACY



Datageest moet terug in de fles



Achtergrond

Privacy en archivering:
bondgenoten of vijanden?

Opinie

Kabinet, stimuleer
encryptie

Praktijk

Op kop met MDTO





06

VISIE

Datageest terug in de fles

Als het nieuwe kabinet echt een nieuwe bestuurscultuur wil, dan zal het de ongezonde datacultuur moeten veranderen.

12

ACHTERGROND

Privacy en archivering

Zitten privacy en archivering elkaar in de weg of zijn het bondgenoten?



20

PRAKTIJK

Op kop met MDTO

Decentrale overheden gaan aan de slag met MDTO om van theorie naar praktijk te komen



16

ACHTERGROND

Gemeenteraad online

Digitale volksvertegenwoordiging werkt, zolang je de risico's maar aanvaardt



22

PRAKTIJK

Schotloos toezicht

Hoe toezichthouders bij de gemeente Amersfoort steeds meer samenwerken



18

PRAKTIJK

Groeien in weerbaarheid

Het Digital Trust Center helpt Nederlandse bedrijven met online weerbaarheid



27

NIEUW IN HET VAK

Anniek van der Pijl

'Stap uit je comfortzone'





05

EDITORIAL
Bart Hekkert

Als donderslag bij heldere hemel



08

COLUMN
Tijs Weustenraad

Privacy van overledenen



10

OPINIE
Rejo Zenger
Kabinet moet encryptie stimuleren

24

SERVICEBERICHT
Week van de Privacy



28

PRIKKEL
Bij de les blijven

28

SERVICEBERICHT
Modernisering van de archiefwet

29

BOEKBESPREKING
BEgrip

30

VERENIGINGSNIEUWS
Toekomst van de archieffunctie

Colofon

Redactieadres
Publiek Denken
Gebouw M1-47,
Binckhorstlaan 36,
2516 BE Den Haag
www.publiekdenken.nl
T 085 486 85 41
E od@publiekdenken.nl

Aanleveren kopij
E od@publiekdenken.nl

Uitgever
Asha Narain

Redactie
Jeroen Jonkers
(hoofdredacteur), Edwin
Driessen, Bart Hekkert,
Eric Kokke, André Plat,
Cynthia Schokker, Migiza
Victoriashoop

Medewerkers aan dit nummer
Simone Driessen, Jeroen
Kasbergen, Chantal Menting,
Rens Ouwerkerk, Kees
Verhoeven, Tijs Weustenraad,
Walter van Wijk, Brenno de
Winter, Rejo Zenger

Beeld- en eindredactie
Marc Notebomer

Art direction en vormgeving
Dimdim Grafisch Ontwerp

Cover
Studio Goudbaard

Beeld
Dimitry de Bruin, John van
Gelder, Shutterstock,

*Adreswijzigingen en
aanvraag abonnementen*
Abonnementsprijs
€ 138, ex btw per jaar
Losse nummers op aanvraag
verkrijgbaar
E od@publiekdenken.nl

Advertenties
MediaSales0031
Boyke Rajbalsing
E boyke@mediasales0031.nl
M 06 109 347 77

Drukker
Damen Drukkers

Od verschijnt 8 x per jaar en
wordt uitgegeven door



De in dit blad verkondigde meningen hoeven niet die van de redactie te zijn. De onafhankelijkheid van de redactie mag niet in het geding komen.

Alle rechten voorbehouden. Niets uit deze uitgave mag worden vervoerd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Volg ons op LinkedIn en Twitter





Hét platform voor de
informatieprofessional
bij de overheid

OD-KALENDER 2022

ADVERTEREN IN OD

Magazine en website

Vakblad en e-zine Overheidsdocumentatie, *Od*, is het netwerkplatform voor informatieprofessionals bij de overheid en de non-profitsector.

Gezien het toenemende belang van digitalisering in onze samenleving wordt het vak voor iedereen die zich met informatievoorziening bezighoudt nóg belangrijker. De urgentie om kennis en ervaringen met elkaar te delen is groot. Met aandacht voor ontwikkelingen in het vakgebied, best practices, samenwerking, persoonlijke ontwikkeling, valkuilen en dilemma's geven wij een kijkje in de keuken van de informatieprofessional bij overheden en de non-profitsector.

Voor meer informatie over adverteren, het meesturen van
bijsluiters en het plaatsen van vacatures:

MediaSales0031

Boyke Rajbalsing

E boyke@mediasales0031.nl

M 06 109 347 77

OD ZOEKT STRATEGISCHE PARTNERS

Od richt zich op informatieprofessionals, informatiemedewerkers, DIV'ers, leidinggevend en teamleiders bedrijfsvoering, automatisering en informatievoorziening bij ministeries, provincies, gemeenten, waterschappen, agentschappen en uitvoeringsorganisaties. Is deze doelgroep ook belangrijk voor u en zoekt u een mogelijkheid uw visie, aanpak, experiment, best practice of dienstverlening bij onze lezers onder de aandacht te brengen? Mail dan naar: od@publiekdenken.nl of kijk op onze website Od-online.nl.



THEMANUMMERS EN VERSCHIJNINGSDATA 2022

Verschijningsdatum Thema

17	28 januari	Preservering
18	25 februari	Security en privacy
19	1 april	AI en beheer
20	20 mei	Toezicht en monitoring
21	24 juni	Arbeidsmarkt in beweging
22	23 september	De gebruiker centraal
23	4 november	Actieplan open op orde
24	2 december	Thema nader te bepalen

OP DE HOOGTE BLIJVEN?

GEEF U OP VOOR ONZE E-NIUWSBRIEF OF MELD U AAN
VOOR EEN (PROEF)ABONNEMENT. MAIL NAAR:
OD@PUBLIEKDENKEN.NL

Od wordt uitgegeven door





Tekst **Bart Hekkert**
Bart Hekkert is redactielid Od

Als donderslag bij heldere hemel

De Belastingdienst heeft jarenlang de privacywet op “ernstige wijze geschonden” door persoonsgegevens van mensen die werden aangemerkt als potentiële fraudeurs bij te houden.’ Waarover dit citaat uit *NRC* van 29 oktober 2021 gaat, behoeft geen verdere uitleg. De toeslagenaffaire is een voorbeeld, misschien wel het voorbeeld bij uitstek, van het schenden van de privacy van betrokkenen door de overheid. Hoewel de weg naar eerherstel en terugbetaling nog maar net is opgestart, zal het nieuwe kabinet vol aan de bak moeten om herhaling te voorkomen.

Hoe kan het dat een overheid – waarvan je mag verwachten dat zij optreedt als hoeder van de rechten van inwoners – jarenlang de privacywetgeving overtrad? En hoe moet de overheid weer terug naar haar taak als hoofdbewaker van de privacy van inwoners? Het nieuwe kabinet lijkt de ernst van deze zaak in te zien en heeft een nieuwe positie gecreëerd voor een staatssecretaris voor Digitalisering. Alexandra van Huffelen zal niet alleen als privacywaakhond moeten acteren, zij zal ook oog moeten hebben voor de dataveiligheid van burgers en bedrijven. Lees hierover ook het artikel “Van Huffelens overvolle agenda: van datacenters tot nepnieuws” in *Het Financieele Dagblad* van 24 januari 2021.

Nederland profiteert bij uitstek van goede kabelverbindingen, datacenters en technisch talent. Dat maakt ons land aantrekkelijk voor bedrijven en investeerders, maar ook voor hackers en kwaadwillende landen. Landen worden ononderbroken aangevallen en vallen elkaar aan (zoek maar eens op *cyber threat map* en verbaas je over de constante stroom met cyberaanvallen). Dat vraagt om goed beleid, strakke beheersmaatregelen en voortdurend toezicht.

Misschien denkt u dat privacyschendingen en cyberaanvallen op deze schaal alleen tussen landen plaatsvinden, maar niets is minder waar. Denk alleen al aan de cyberaanval op de gemeente Hof van Twente in december 2020: ‘De aanval op de gemeente kwam voor het college als een donderslag bij heldere hemel,’ zo schreef Brenno de Winter in zijn duidingsrapport *Te goed van vertrouwen?*. En dan is deze hack nog landelijk nieuws. Wees eens eerlijk: hoe vaak overtreedt uw bestuursorgaan privacywetgeving, worden gegevens te lang bewaard, en hoe is het gesteld met de data- en informatiebeveiliging?

In dit nummer aandacht voor een breed scala aan invalshoeken op het thema security en privacy. Chantal Menting, plaatsvervangend gemeentearchivaris, schrijft hoe in de gemeente Amersfoort vier toezichthouders de organisatie scherp houden op planning & control, privacy, beveiliging en opslag & archivering. Het belang van bescherming van privacy en van beveiliging van data wordt toegelicht in een bijdrage van Kees Verhoeven. Dat we hierbij niet alleen aan opslag moeten denken maar bijvoorbeeld ook aan onze communicatie, wordt extra duidelijk in het artikel over encryptie, geschreven door Rejo Zenger. Gelukkig wordt de ambtenaar ook via webinars scherp gehouden op privacy en security. Walter van Wijk schrijft een korte samenvatting van de presentaties tijdens de Week van de Privacy (met handig links naar podcasts en webinars).

Laat u inspireren door de bijdragen in dit themanummer en kijk wat u kunt doen binnen uw gemeente, rijksorganisatie of waterschap om de privacy van burgers te waarborgen en data veilig buiten bereik van criminelen te houden. Laat uw donderslag niet bij heldere hemel komen.

Tekst **Kees Verhoeven**Kees Verhoeven is voorzitter van de
raad van advies van de KNVI

Maak verschil tussen surveillance- en democratische rechtsstaat

Datageest moet terug in de fles

Terwijl we ons vandaag de dag druk maken over de toenemende datamacht van bedrijven als Facebook en Amazon, cyberspionage vanuit China en desinformatie uit Rusland, staan onze vrijheid en veiligheid ook van binnenuit onder druk. Want ook democratisch gekozen regeringen kruipen met digitale middelen en databestanden steeds dieper onder de huid van burgers. Hoewel dat grotendeels met goede bedoelingen gebeurt, om narigheid te voorkomen, beweegt ook Nederland zich geleidelijk van een rechtsstaat naar een surveillancestaat waarin het individu minder privacy heeft. Als het nieuwe kabinet echt een nieuwe bestuurscultuur wil, dan zal het ook de ongezonde datacultuur moeten veranderen.



Afgelopen decennia hebben we aan den lijve ondervonden dat digitale technologieën als computers, het internet, smartphones en kunstmatige intelligentie van grote invloed zijn op menselijk gedrag en dus de samenleving als geheel. Kijk maar eens naar een film uit de jaren tachtig en je ziet hoe intensief onze leefwereld gewijzigd is. “Aan den lijve” mag daarbij letterlijk genomen worden want de persuasieve technologie en sluwe algoritmes van bedrijven als Booking.com en Netflix zorgen voor fysieke reacties die ons brein – onbewust – doet besluiten direct door te klikken naar het volgende aanbod. Ook de gezichtsherkenningcamera's die de volksrepubliek China inzet tegen de Oeigoeren heeft fysieke gevolgen voor deze onderdrukte minderheid.

Nieuwe olie

Wanneer het gaat over machtsverschuiving als gevolg van digitale technologie, dan gaat het al snel over autocratische leiders als Poetin, Erdoğan of Xi Jinping. Of over de door figuren als Jeff Bezos en Mark Zuckerberg ontworpen verdienmodellen waarmee big tech miljarden verdient. Namelijk door kleine zelfstandigen oneigenlijk te beconcurreren of door mensen zolang mogelijk op hun platform te houden met opruiende, polariserende of zelfs discriminerende en intimiderende content. Alles voor de ongedeelde macht. Alles voor het grote geld.

Deze machtsposities zijn terug te voeren op de periode rond het symbolische sleuteljaar 2000, toen het mondiaal internetoptimisme op zijn hoogtepunt was. Terwijl Vladimir Poetin in Rusland het roer had overgenomen van Boris Jeltsin, deed de Amerikaanse president Bill Clinton de even naïeve als overmoedige bewering dat het controleren van het – zo bevrijdende en democratiserende – internet hetzelfde was als een poging om een plumpudding tegen de muur te spijkeren.

En terwijl commentatoren en deskundigen zich maanden hadden blindgestaard op de voorspelde *millennium-bug* brak kort daarop de onvoorziene dotcomcrisis uit, die de eerste generatie internetbedrijven dwong om de

'EEN HERHALING VAN DE ONMENSELIJKE TOESLAGENGESCHIEDENIS IS EEN KWESTIE VAN TIJD'

'EEN OVERHEID DIE DE WET OVERTREEDT, PAST NIET BINNEN DE NEDERLANDSE RECHTSORDE'

internetzeepbel in te ruilen voor een hard verdienmodel. Gebaseerd op data, die zo de nieuwe olie werden.

EVRM

Wat we vaak vergeten en wat we ook veel minder goed konden waarnemen, was het ontstaan van een derde digitale machtspositie. In 2001 leidden de aanslagen van 9/11 namelijk niet alleen tot de befaamde *war on terror* van president George W. Bush maar ook tot het op grote schaal - maar heimelijk - verzamelen van persoonlijke data door regeringen van democratische rechtsstaten. Lang bleef deze praktijk onder de oppervlakte maar na de onthullingen in 2013 van oud-CIA- en NSA-medewerker Edward Snowden werd duidelijk dat haast alle westerse regeringen aan massale surveillance deden.

Hoewel er destijds veel kritische reacties kwamen en politici op hun achterste benen stonden, is deze datageest nooit meer de fles terug in gegaan. Nederland vormt op deze regel geen uitzondering.

De afgelopen jaren is pijnlijk duidelijk geworden welke consequenties dit heeft voor het functioneren van onze rechtsstaat. Om fraude te bestrijden maakte de Belastingdienst jarenlang gebruik van een zogeheten Fraude Signalering Voorziening (FSV) dat uitmondde in een zwarte lijst vol onschuldige burgers. Inmiddels hebben verschillende onderzoeken uitgewezen dat deze werkwijze alle perken te buiten ging. Een vergelijkbaar - op bijstandsfraude gericht - datasysteem van het ministerie van Sociale Zaken, Systeem Risico Indicatie geheten, werd ondanks veel protesten pas stilgezet toen een rechter het begin 2020 verbood, omdat de wetgeving erachter in strijd was met het Europees Verdrag voor de Rechten van de Mens (EVRM).

Buiten wettelijke kaders

Deze dure lessen ten spijt publiceerde het ministerie van Justitie en Veiligheid de Wet gegevensverwerking door samenwerkingsverbanden (WGS), die honderden overheidsinstanties de mogelijkheid biedt om talloze



Tekst **Tijs Weustenraad**

Tijs Weustenraad is jurist intellectuele eigendom,
ict-recht en privacy bij Elferink & Kortier Advocaten

Privacy van overledenen

Stel, bij de balie van uw archief meldt zich een persoon die inzage wil in gegevens van iemand uit zijn gemeente. Over die persoon gaat in de gemeenschap een hardnekkig gerucht dat hij lid van de NSB zou zijn geweest en degene aan de balie wil dat gerucht nader onderzoeken. De persoon in kwestie is inmiddels overleden. Hoe gaat u om met dit verzoek? Geeft u inzage?

Uiteraard gaat u eerst na of er openbaarheidsbeperkingen zijn gesteld. En zo ja, of er opheffing mogelijk is. Maar naast de openbaarheidsbeperkingen op grond van de Archiefwet, speelt de Algemene verordening gegevensbescherming (AVG) een rol. Deze geeft regels over de verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die direct of indirect iets zouden kunnen zeggen over een natuurlijk persoon. Natuurlijk persoon, dat is juristentaal voor: iemand die nog leeft. De AVG is dus niet van toepassing op gegevens van overledenen. Dat klinkt logisch, maar is toch te snel door de bocht. Het is een misvatting om ervan uit te gaan dat u geen rekening meer hoeft te houden met de privacy van de overledene. Hoe zit dat? Allereerst kunnen gegevens over een overledene ook iets zeggen over zijn nog levende nabestaanden. Denk bijvoorbeeld aan een foto waar het hele gezin op staat of een adres waarop de nabestaanden nog steeds wonen. In dergelijke gevallen zijn de gegevens over de NSB'er tegelijkertijd persoonsgegevens van de nabestaanden. Bovendien is het gegeven dat hun vader al dan niet een NSB'er is geweest direct op de nabestaanden van toepassing. Met andere woorden: die informatie is op zichzelf een persoonsgegeven van de nabestaanden omdat het iets zegt over die nabestaanden. Op verwerking van dergelijke gegevens zijn de regels van de AVG wel van toepassing. De nabestaanden zijn dan degenen die het aangaat.

Bij foto's en andere beeldmaterialen zou er verder sprake kunnen zijn van portretrechten. Een portret is een afbeelding waarop iemand herkenbaar is afgebeeld. Voor openbaarmaking van in opdracht gemaakte portretten is tot 10 jaar na het overlijden van de geportretteerde toestemming vereist van alle nabestaanden. Gaat het om niet in opdracht gemaakte portretten, dan kunnen de nabestaanden zich verzetten tegen de openbaarmaking van het portret, voor zover zij daarbij een "redelijk belang" hebben. Wat een redelijk belang is, is in rechtspraak uitgewerkt. Denk bijvoorbeeld aan het belang om onder bepaalde omstandigheden een onverstoord nagedachtenis te hebben aan de overledene of het geval dat de openbaarmaking van het portret zou kunnen leiden tot bespotting.

Tot slot kent ons rechtstelsel het algemene leerstuk van de onrechtmatige daad. Het openbaren, verspreiden of anderszins verwerken van bepaalde informatie zou onder omstandigheden een onrechtmatige daad jegens de nabestaanden kunnen zijn. Wanneer dat het geval is, is niet op voorhand te zeggen. Een en ander hangt af van de specifieke omstandigheden van het geval. Denk aan situaties waarbij de eer of de goede naam van de overledene of diens nabestaanden wordt aangetast.

Toch een geruststellend idee dat ook de doden een zeker recht op privacy hebben.

De advocaten en juristen van Elferink & Kortier Advocaten schrijven een column, waarin zij een praktisch probleem op het gebied van de AVG in relatie tot informatiebeheer behandelen. Heeft u een praktijkvraag die u behandeld wilt zien? Stuur deze naar Od@publiekdenken.nl.

databestanden uit te wisselen en te verwerken. Dit betekent dat de overheid in potentie een datadeeltjes-versneller optuigt waarmee op grote schaal conclusies over burgers getrokken kunnen worden: hoe meer bestanden je aan elkaar koppelt, hoe meer gegevenscombinaties je kunt vormen en hoe meer analyses je kunt maken. Omdat deze haast onbegrensde mogelijkheden lang niet altijd leiden tot juiste conclusies over mensen, lijkt een herhaling van de onmenselijke toeslagengeschiedenis een kwestie van tijd.

Ook de bestuurlijke wens tot het voorkomen van terroristische aanslagen, het bestrijden van kindermisbruik of het indammen van de coronapandemie leidde tot de inzet van uiteenlopende data-oplossingen in de vorm van de sleepwet, de hackwet en de Corona-app. Omdat deze voorstellen uiteindelijk - na felle discussies en zelfs een referendum - werden aangenomen door de Staten-Generaal past de wetgeving binnen de uitgangspunten van de democratische rechtsstaat. Zorgelijk genoeg geldt dit niet voor de op data gebaseerde uitvoering. In de afgelopen jaren is uit onderzoek van onderzoeksjournalisten, wetenschappers, burgerrechtenorganisaties, toezichthouders en adviesorganen gebleken dat een reeks overheidsorganisaties buiten de wettelijke kaders is getreden.

Hierbij gaat het bijvoorbeeld om de inlichtingendiensten (AIVD en MIVD), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Nationale Politie. Steeds was in deze gevallen sprake van een goedbedoelde surveillance-activiteit zonder wettelijke bevoegdheid of in strijd met grondrechten en/of internationale verdragen.

Tegenspraak

Een overheid die de wet overtreedt, past niet binnen de Nederlandse rechtsorde. Dat het met goede bedoe-

'BESTUURDER EN INFORMATIEPROFESSIONAL MOETEN BETER NAAR ELKAAR LUISTEREN'

lingen gebeurt, doet daar niets aan af. In het belang van ons allemaal komt er verandering in deze situatie. Het kersverse kabinet stelt zichzelf ten doel om te komen tot een nieuwe bestuurscultuur en een versterking van de rechtsstaat. Dit gaat niet lukken zonder hierin de zo invloedrijke - maar nog steeds schromelijk onderschatte - datacultuur te betrekken.

De nieuwe staatssecretaris voor Digitalisering kan hierbij de regie nemen en zo het verschil maken tussen een surveillancestaat en een democratische rechtsstaat. Hierbij kan ze natuurlijk niet zonder de hulp van alle IT- en informatieprofessionals, die zowel binnen als buiten de overheid dagelijks bezig zijn om data- en informatiesystemen op duurzame wijze in te zetten. Wat zou het mooi zijn als er over 3 jaar een Publiek Data Kader (PDK) van de staatssecretaris ligt waar alle ministeries zich bij hun dataprocessen aan houden. Om deze ambitieuze operatie te laten slagen is wel intensieve samenwerking nodig. Enerzijds moeten bestuurder en informatieprofessional beter naar elkaar luisteren om de bestuurlijke invalshoek en de specialistische visie meer te laten samenvallen dan nu het geval. Anderzijds is deskundige tegenspraak juist nodig om het gevaar op tunnelvisie en groepsdenken te verkleinen. Ik wens alle betrokkenen vanaf deze plek heel veel succes bij hun cruciale taak.

Tekst **Rejo Zenger**

Rejo Zenger werkt als beleidsadviseur bij Bits of Freedom

Weg met stiekem meekijken

Kabinet moet encryptie stimuleren

Het nieuwe regeerakkoord benadrukt wat we al lang weten: de digitale revolutie biedt geweldige kansen voor onze samenleving en economie. De keerzijde wordt gelukkig ook gezien, want ook onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen staan onder druk, aldus het akkoord. Daarom is het belangrijk dat het nieuwe kabinet inzet op bewezen technologie die ons beschermt. De overheid moet actief de ontwikkeling, de beschikbaarheid en de toepassing van encryptie stimuleren.

Encryptie is een manier om gegevens te beschermen door ze onleesbaar te maken voor ieder ander dan de bedoelde ontvanger. Als je via WhatsApp een berichtje stuurt, wordt het berichtje op jouw telefoon versleuteld en is het alleen nog leesbaar te maken op de telefoon van de ontvanger. Dat onleesbaar maken gebeurt door een wiskundig proces. De rekensom die de app daarin moet maken noem je het algoritme. Een sterk algoritme is een rekensom die zo moeilijk is dat je die alleen kunt oplossen als je ook over de sleutels beschikt. Of over een onrealistische berg computerkracht. Met goede encryptie zijn gegevens dus veilig opgeborgen. En dat maakt encryptie zo geschikt voor dagelijks gebruik. De toepassing is breed, denk bijvoorbeeld aan internet-bankieren. Het zorgt er bijvoorbeeld voor dat je zeker kunt zijn dat je met je eigen bank zakendoet en niet

met een partij die zich valselyk voordoe als jouw bank (authenticiteit). Encryptie zorgt er voor dat niemand stiekem kan meekijken naar wie jij geld overmaakt omdat de transactie voor een buitenstaander onleesbaar is (vertrouwelijkheid). Encryptie zorgt ervoor dat niemand onderweg jouw betaalopdracht kan aanpassen waardoor je geld alsnog bij de verkeerde terecht komt (integriteit). Tenslotte, door jouw gegevens versleuteld op te slaan kan de bank ervoor zorgen dat bij een digitale inbraak niet alles op straat komt te liggen.

Eindeloos

De ontwikkeling, beschikbaarheid en toepassing van encryptie zijn fundamenteel voor de bescherming van onze digitale infrastructuur en communicatie. Het is niet alleen essentieel voor de autonomie van mensen in onze democratische rechtsstaat, maar net zo goed

'ENCRYPTIE IS CRUCIAAL OM ONZE DIGITALE INFRASTRUCTUUR TE BESCHERMEN'

voor innovatie en economische groei. Vandaag de dag vertrouwt iedereen, vaak onbewust, op encryptie. Ook de overheid doet dat.

Zonder encryptie kan zij haar burgers niet vragen online belastingaangifte te doen. De technologie stelt de overheid in staat om gevoelige zaken veilig te bespreken met haar ambassadepersoneel in het buitenland. Het maakt het mogelijk om op betrouwbare manier te communiceren met burgers in tijden van een crisis, zoals een pandemie. De geheime diensten versleutelen staatsgeheim om zich te beschermen tegen hacks van statelijke actoren. Encryptie draagt bij aan de integriteit van onze verkiezingen. Of om er zeker van te zijn dat alleen rechercheurs kennisnemen van de informatie in een opsporingsonderzoek. Waterschappen gebruiken encryptie om de toegang tot de beheerinterface van gemalen te beveiligen. De lijst is eindeloos.

Iedereen vertrouwt erop

Niet alleen de overheid vertrouwt op encryptie. Deze technologie stelt ook inwoners in staat om met elkaar hun intiemste gedachten te delen, om een laptop in de trein te vergeten zonder al te grote risico's te lopen en om veilig online aankopen te doen. En van dat vertrouwen profiteren bedrijven natuurlijk ook weer. Bedrijven die op hun beurt ook weer zelf op encryptie vertrouwen. De toepassing van encryptie is een van de manieren om zich te wapenen tegen economische spionage. Maar ook als democratische samenleving als geheel vertrouwen we op encryptie. Het stelt ons in staat om in vrijheid informatie te vergaren en te delen. En journalisten vertrouwen erop voor de bescherming van hun onderzoek en bronnen.

Deze duidelijke behoefte aan encryptie wordt breed gevoeld. Minder dan een jaar geleden bracht Bits of Freedom, samen met andere belanghebbenden, een publieke oproep naar buiten waarin het nieuwe kabinet wordt aangespoord encryptie te stimuleren. Die werd ondertekend door een ongekend brede groep uit alle hoeken van de samenleving. Een "monsterverbond" volgens het *Het Financieele Dagblad*. In de lijst

vind je organisaties die opkomen voor de belangen van consumenten en kinderen, vertegenwoordigers van journalisten en mediabedrijven, bedrijven die de digitale infrastructuur in Nederland beheren, experts in de beveiliging daarvan, mensenrechtenorganisaties en organisaties die onze onderwijsinstellingen voorzien van internet. Maar ook organisaties en deskundigen die de overheid gewoonlijk helpen met het aftappen van telefonie- en internetverbindingen ondertekenden onze oproep. Iedereen is het er over eens: het kabinet moet encryptie stimuleren.

Rol van overheid

Het kabinet erkende dat ook en acht het sinds 2016 onwenselijk om wettelijke beperkingen op de ontwikkeling, de beschikbaarheid en de toepassing van encryptie te introduceren. Toch is er van tijd tot tijd altijd weer een enkeling die vindt dat het anders moet. Dat is goed te begrijpen: echt iedereen vertrouwt op encryptie. Ook criminelen. Zij hebben immers ook de behoefte om hun informatie te beschermen tegen pottenkijkers. Dat maakt het werk van opsporings- en geheime diensten een stuk moeilijker, dat zal niemand ontkennen. Maar juist omdat encryptie zo'n belangrijke rol in de bescherming van onze digitale infrastructuur speelt, en daarmee in onze democratische rechtsstaat en onze economie, moet het kabinet inzetten op alternatieve interventies. Niet blindstaren op wat niet (meer) kan, maar kijken naar de middelen die we wel hebben. En er voor zorgen dat die ten volste kunnen worden benut. Sleutelen aan encryptie betekent dat we een van de weinige middelen ondermijnen die onze informatie kan beschermen. Dat kunnen we ons niet veroorloven. Niet als individu, niet als bedrijfsleven, niet als democratische rechtsstaat, maar ook zeker niet als overheid. Het kabinet moet daarom juist de ontwikkeling, de beschikbaarheid en de toepassing van encryptie actief stimuleren. En wie kan dat beter uitleggen dan die ambtenaren die zich dagelijks en professioneel bezighouden met de beveiliging van informatie en informatiestromen?

'OOK CRIMINELEN VERTROUWEN OP ENCRYPTIE'

Tekst **Rens Ouwerkerk**

Rens Ouwerkerk is senior adviseur informatiebeheer bij de gemeente Amsterdam en momenteel gedetacheerd bij het Nationaal Archief als adviseur kennisproducten



Privacy en archivering

Vijanden of bondgenoten?

In de AVG staat de wettelijke plicht om *privacy by design* toe te passen. Ook zetten overheidsorganisaties in op *security by design*, *open by design*, archivering *by design* en ethiek *by design*. Zitten deze concepten elkaar niet in de weg? Of valt dat mee en versterken ze elkaar? Laten we in dit themanummer eens nader stilstaan bij de thema's privacy, openbaarheid en archivering *by design*.

'WE HOUDEN ONVOLDOENDE REKENING MET ZOWEL PRIVACYBESCHERMING ALS DUURZAME TOEGANKELIJKHEID'

Regelmatig hoor ik collega's roepen dat privacy en archivering tegengestelde belangen dienen. Archivering is gericht op het toegankelijk en openbaar maken van informatie, terwijl privacybescherming juist gericht is op het afschermen van informatie. Wat mij betreft is dit een schijn-tegenstelling. Ik ken namelijk geen enkele informatiebeheerder die vindt dat de overheid massaal de privacy van burgers moet schenden en terabytes met gevoelige gegevens op straat moet gooien. Ik ken ook geen enkele *privacy officer* die tegen een transparante overheid is en vindt dat alles stiekem en in het geniep moet plaatsvinden. Kortom, het is niet zo zwart-wit. Waar komt dan dat gevoel vandaan dat deze perspectieven elkaar in de weg zitten? Misschien heeft dat te maken met de onhandige manier waarop we onze informatiehuishouding tot nu toe hebben ingericht. We hebben in het ontwerpen van ons informatielandschap namelijk onvoldoende rekening gehouden met zowel privacybescherming als duurzame toegankelijkheid. Het gevolg? Bij een Wob-verzoek moeten we grote hoeveelheden documenten handmatig lakken om aan privacy-wetgeving te voldoen. Veel werk,

veel gedoe en dus gemopper op de werkvloer. En gemopper bij de aanvrager dat het allemaal wel erg lang duurt: heeft de overheid soms iets te verbergen? Kortom: het probleem is niet zozeer dat we met tegengestelde belangen te maken hebben, het probleem is dat we onvoldoende *by design*-maatregelen hebben getroffen om recht te doen aan die verschillende perspectieven.

Anonimiseringssoftware

De oplossing voor het genoemde lakprobleem ligt voor de hand: overheden zetten massaal in op *tools* waarmee ze automatisch persoonsgegevens kunnen herkennen en weglakken. Dankzij zelflerende algoritmes kunnen deze *tools* dit rotklusje steeds autonomer en steeds accurater van ons overnemen, zodat wij onze kostbare tijd kunnen besteden aan leuke dingen. Toch is dit maar een deel van de oplossing. Het onderliggende probleem is dat we structureel informatie creëren in een vorm die niet geschikt is om openbaar te maken. Om dat op te lossen, gaan we achteraf documenten "verminken" met laksoftware. Terwijl we ons informatielandschap ook *by design* zo kunnen inrichten dat onze systemen automatisch twee documentversies kunnen uitspugen: een volledige versie voor intern gebruik en een publicatieversie zonder persoonsgegevens. Een bekend voorbeeld is het Omgevingsloket. Een aanvrager vult gegevens in, die landen in een database en het systeem weet welke gegevens openbaar zijn en welke niet. Zo kunnen we geautomatiseerd een

publicatieversie maken. En hebben we helemaal geen ingewikkelde AI-oplossingen nodig om achteraf de boel te anonimiseren. Een mooi voorbeeld van hoe *privacy by design* bij kan dragen aan actieve openbaarmaking. Gelukkig gaat de vernieuwde Wet hergebruik van overheidsinformatie ons straks verplichten om te zorgen dat informatie wordt 'ontworpen, vervaardigd en beschikbaar gesteld op een manier die openheid en hergebruik van die documenten toegankelijk en gemakkelijk maakt'.¹

Slim

Ook vanuit archiveringsperspectief is het slim om dit soort oplossingen te bedenken. Als we onze datamodellen handig inrichten, hoeven we immers niet langer verschillende versies van documenten te bewaren. We bewaren gewoon de data met het datamodel en kunnen daarmee op elk gewenst moment de ene of de andere versie van een document als *view* op die data aanbieden. De techniek is al volop voorhanden, maar we staan het onszelf nog onvoldoende toe om daar gebruik van te maken omdat ons paradigma gebaseerd is op het concept van het document als een gefixeerde eenheid van gegevens. Ik betoogde 2 jaar geleden al eens in dit blad dat we minder in documenten moeten gaan denken.² De vraag zou veel meer moeten zijn: hoe zorgen we dat we verschillende *views* op data mogelijk

¹ Concept wetsvoorstel Wet implementatie open data richtlijn d.d. 23-12-2021, artikel 5 lid 1.

² Rens Ouwerkerk, 'Van documenten en de dingen die voorbij gaan', *Od* jaargang 74, nr. 1, januari 2019 pp. 15-17.

Ambtenarenpanel

REFLECTIE OP DE OVERHEID



Wilt u ook
weten wat
ambtenaren
vinden?

Maak dan gebruik van Ambtenarenpanel!

Stuur een e-mail naar info@ambtenarenpanel.nl

Ambtenarenpanel

is een samenwerking van



TOP
ONDERZOEK
WEET WAT ER GEBEURT.

'DOOR MEER IN TERMEN VAN GEGEVENS TE DENKEN KUN JE DE BRUG NAAR PRIVACYBESCHERMING SLAAN'

maken en door de tijd heen kunnen reproduceren? En veel minder: hoe zorgen we dat we elke ooit gecreëerde *view* als gefixeerd document kunnen bewaren? Door meer in termen van gegevens te denken, is het gemakkelijker om de brug naar privacybescherming te slaan en tot integrale oplossingen te komen. Persoonsgegevens zijn immers gegevens en geen documenten.

Tijdige vernietiging

Nu we hebben vastgesteld hoe *privacy by design* helpt om openbaarheid te stimuleren, is de vraag gerechtvaardigd hoe dat andersom is. Wat hebben die privacydeskundigen eigenlijk aan informatiebeheerders en archiefspecialisten? Een belangrijke raakvlak is tijdige vernietiging. De AVG schrijft voor dat persoonsgegevens niet langer bewaard mogen blijven dan noodzakelijk, maar beschrijft niet hoe je dat precies moet regelen. De Archiefwet doet dat wel en biedt daarmee een welkome aanvulling op de AVG. Mits er bij het opstellen van selectielijsten voldoende rekening wordt gehouden met het privacyperspectief, is het een praktisch instrument waar zowel informatiebeheerders als privacyspecialisten mee geholpen zijn.³

³ KIA-werkgroep AVG, *Weten of vergeten: Handreiking voor het toepassen van de Algemene verordening gegevensbescherming in samenhang met de Archiefwet in de dagelijkse praktijk van het informatiebeheer bij de overheid* (april 2020).

Bijkomend voordeel: als informatie waarvan het belang is verstreken netjes op tijd wordt vernietigd, dan hoeft die ook niet meer doorgespit te worden bij een Wob-verzoek. Natuurlijk zitten er ook persoonsgegevens in documenten die eeuwig bewaard blijven. Door informatie als *view* op data in te richten, regelen we dat voor blijvend te bewaren informatie een volledige *view* pas weer mogelijk is na het verstrijken van alle openbaarheidsbeperkingen.

Samenwerking in de praktijk

Onlangs interviewde ik voor de *Handreiking Archivering by Design* van het Nationaal Archief (houd hiervoor de website van het Nationaal Archief in de gaten!) een adviseur informatiebeheer bij een Brabantse gemeente over diens praktijkervaringen. Hij vertelde dat hij optrok met zijn privacycollega's omdat ze een gedeelde uitdaging hadden: vanaf het begin betrokken worden bij IT-projecten om zo *by design* hun bijdrage te kunnen leveren. Beide vakdisciplines werden voorheen nog weleens niet of pas te laat betrokken. Inmiddels hebben ze het interne proces zo ingericht dat zowel de privacydeskundigen als de informatiebeheerders standaard aangehaakt worden als een nieuw project start. Allereerst is dit natuurlijk een mooi voorbeeld van hoe het aangaan van bondgenootschappen kan helpen om in positie te komen, maar bovenal illustreert het dat de vermeende tegenstelling op de werkvloer helemaal niet zo ervaren wordt.

Achteraf reparatiewerk

Ik herken dit ook vanuit mijn eigen praktijk de afgelopen jaren. Wat

me daarbij opviel, was dat de privacyspecialisten in mijn omgeving erg sterk waren in de procedurele aspecten. Zoals het vastleggen van afspraken in een verwerkersovereenkomst. Voor de praktische vertaling naar systeemrichting, was daarentegen minder aandacht. Voor ons als adviseurs informatiebeheer gold eigenlijk het omgekeerde: wij waren juist sterk in de systeemrichting, maar hadden geen gezaghebbende formats als PIA's (Privacy Impact Assessment) en VWO's (Standaard Verwerkersovereenkomst). Daarin vulden we elkaar dus aan. De privacyspecialisten voelden zich gesteund doordat wij ze werk uit handen namen. Ze hoefden niet meer zelf uit te zoeken hoe dat nu eigenlijk zit met bewaartermijnen. Wij voelden ons weer gesteund doordat we ons verhaal kwijt konden in de gezaghebbende documentatie van de *privacy officers*. Al met al is de conclusie gerechtvaardigd dat privacy, archivering en openbaarheid elkaar niet in de weg zitten. Sterker nog: intensieve samenwerking is een absolute voorwaarde om transparantie en openbaarheid te bewerkstelligen. De vakdisciplines bieden verschillende perspectieven op dezelfde vraagstukken en vullen elkaar aan. Dan moeten we echter wel *by design* en in onderlinge samenhang de juiste maatregelen treffen in plaats van enkel achteraf reparatiewerk verrichten.

'INTENSIEVE SAMENWERKING IS EEN ABSOLUTE VOORWAARDE OM OPENBAARHEID TE BEWERKSTELLIGEN'

Tekst **Brenno de Winter**

Brenno de Winter is chief security and privacy operations, programma Realisatie Digitale Ondersteuning, bij het ministerie van VWS

Aanvaard de risico's

Digitale volksvertegenwoordiging werkt

Er zit wetgeving in de pijplijn die het mogelijk maakt dat vergaderingen van gemeenteraden en provinciale staten op structurele basis online kunnen plaatsvinden. Al gaat er weinig boven elkaar fysiek zien, toch is dat een geweldige kans. Tenzij we opnieuw wegduiken voor de risico's die onlosmakelijk aan technologie verbonden zijn.

Als we iets aan de coronapandemie te danken hebben, is het wel het digitaal vergaderen. Wie met meerdere organisaties in verbinding staat, heeft een arsenaal aan applicaties geïnstalleerd: Zoom, Microsoft Teams, BlueJeans, WebEx, Jitsi, en ga zo maar door. Als de onthullingen van Edward Snowden uit 2015 nog de praktijken van vandaag weerspiegelen, dan heeft vertrouwelijkheid door deze beweging een totaal nieuwe dynamiek gekregen.

Lager spionagerisico

Gelukkig is dat voor het wetsvoorstel voor online

vergaderen door gemeenteraden en provinciale staten niet echt een groot probleem. De meeste vergaderingen van een volksvertegenwoordiging zijn door hun aard immers al openbaar. Niet voor niets is het bij veel gemeenten al gebruikelijk de raadsvergadering via de website te streamen. Dat de input niet uit een raadszaal maar uit een werkkamer komt, is niet een heel grote verandering voor de burger. Waar digitaal vergaderen voor vertrouwelijke informatie een groot risico kan zijn, is dat hier minder het geval.

Dat voordeel betekent dat het eenvoudiger is om dingen te doen, die eerder niet konden. Denk aan een

'VERGADERECHANOLOGIE MAAKT HET DEMOCRATISCH PROCES KWETSBAARDER'

raads- of statenvergadering tijdens een reces, zonder dat iedereen van vakantie hoeft terug te komen. Of een hoorzitting met mensen op afstand. Na de hack op de gemeente Hof van Twente was dat een zegen, omdat de agenda en reisafstand echt niet te matchen waren. Vergaderetechnologie maakt het democratisch proces wel kwetsbaarder. Wanneer een kritisch raadslid op het juiste moment door ransomware wordt getroffen of er een grote DDoS-aanval of een andere gerichte aanval wordt uitgevoerd, komt meteen de democratie in het gedrang. Dat kan ook bij een fysieke vergadering, maar in veel gevallen leiden we dat in goede banen. Digitaal is dat ingewikkelder en lukt het vaak om anoniem te blijven. Met goede timing zijn de scenario's van verstoring van het proces niet ondenkbaar. Dat is een kwetsbaarheid.

Zeker in de fase waarin veel mensen nog aan de techniek moeten wennen. Dat werd wel duidelijk toen een met Zoom opgezette raadsvergadering van de gemeente West Betuwe werd verstoord. Een bezoeker had de mogelijkheid te spreken en maakte daar gretig gebruik van door allerlei racistische en pornografische uitingen rond te strooien. De onmacht en paniek onder de raadsleden maakte duidelijk dat training op zijn plaats is, maar ook hoe eenvoudig het verstoren van een vergadering (en dus de democratie) is.

Deepfake

Die kwetsbaarheden worden groter als niet de technologie, maar het democratisch proces wordt aangevalen. In de fysieke, meerdimensionale wereld herkennen wij dat doorgaans goed. Maar toen een Tweede Kamer-commissie dacht een gesprek te hebben met Nalvalny's rechterhand Leonid Volkov, bleken ze in werkelijkheid te spreken met pro-Kremlingrapenmakers. De rare antwoorden wekten argwaan, niet het beeld van de persoon. Precies een tactiek die de Russen goed uitkwam.

Wie het spel goed speelt, regelt meteen een juiste achtergrond bij de politicus. De meeste vergadersoftware kent de mogelijkheid de achtergrond te vervangen. Een

functie die ik gretig met sommige collega's en vrienden gebruik om te doen of we in elkaars woning zijn. Het enige wat nodig is: dat iemand kort opstaat en uit beeld gaat voor een screenshot. Juist het verschijnsel dat dit soort technologie snel in kwaliteit verbetert, werkt niet in ons voordeel.

Maatregelen nemen

Er is niet veel fantasie nodig om te beseffen dat deepfake-technologie in verkeerde handen een raads- of statenvergadering flink kan verstoren. Tot het punt waarop een stemming te beïnvloeden is. Een eenmaal uitgebrachte stem terugdraaien met het argument dat een sessie was gekaapt kan interessant worden: wil deze gekozen zijn of haar stem toch veranderen als spijtoptant of is er werkelijk meer aan de hand? Het mechanisme om stemmen uit te brengen moet goed worden doordacht.

Dat gaat over de vraagstukken: wat kunnen we online doen en waar is het toch beter om fysiek bij elkaar te komen? Daarnaast helpt het nadenken over waarborgen voor de meest kwetsbare onderdelen van het democratisch proces: bijvoorbeeld het uitbrengen van de stem als volksvertegenwoordiger. Opnieuw biedt de technologie hier goede mogelijkheden om de risico's fors te beperken en beschikken we in Nederland over geschikte infrastructuur om deze oplossingen te realiseren.

Het begint met de aanvaarding dat technologie inherente zwakheden heeft, waartegen we maatregelen moeten nemen. Daaronder ligt een fundamentele discussie: willen we digitaal om het proces te verbeteren of is het een verkapt bezuinigingsoperatie? In het eerste geval zullen de maatregelen de oplossing uiteindelijk beter maken. In het tweede geval is het lastiger voet aan de grond te krijgen om de risico's überhaupt te lijf te gaan.

'WE MOETEN AANVAARDEN DAT TECHNOLOGIE INHERENTE ZWAKHEDEN KENT'

Tekst **Jeroen Kasbergen**

Jeroen Kasbergen is cyber security adviseur bij het Digital Trust Center van het ministerie van Economische Zaken en Klimaat

Digital Trust Center helpt ondernemend Nederland

Groeien in weerbaarheid

Het Digital Trust Center (DTC) gelooft dat digitaal weerbare bedrijven beter in staat zijn om de kansen en uitdagingen te benutten. Om bedrijven daadwerkelijk te laten groeien in weerbaarheid, heeft het DTC een pallet aan diensten ontwikkeld dat ondernemers basisvaardigheden aanreikt en informatie geeft over onderwerpen als phishing, ransomware en de beveiliging van je netwerk. Door middel van online tools, het waarschuwen van individuele ondernemers in het geval van een bij hen geconstateerde kwetsbaarheid en het stimuleren van samenwerking, draagt het DTC bij aan een digitaal weerbare economie.

Het DTC is in 2018 opgericht naar aanleiding van een Tweede Kamer-motie.¹ Op basis van de doelgroep, ondernemend Nederland, is besloten om het DTC onder te brengen bij het ministerie van Economische Zaken en Klimaat. Een van de eerste resultaten van het DTC was het opstellen van de vijf basisprincipes van digitaal weerbaar ondernemen (zie kader). Deze basisprincipes zijn, tot op de dag van vandaag, de kern van de boodschap van het DTC.

Het belang van samenwerking

Vanwege de omvang van de taak - in 2018 waren er ongeveer 1,6 miljoen ondernemers, in 2022 zijn dat er bij-



na 2 miljoen - is samenwerking met partners gezocht. Organisaties zoals VNO-NCW en MKB-Nederland, de Kamer van Koophandel (KvK), het Centrum Informatiebeveiliging en Privacybescherming (CIP-overheid), ECP, Cybersecurity Alliantie (CSA), het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en NLdigital zijn van groot belang om de weerbaarheidsboodschap bij ondernemers te krijgen. Het DTC heeft daarom een gerichte subsidieregeling voor initiatieven die deze weerbaar-

heid vergroten. Maar ook zoekt het DTC actief de samenwerking met andere branchespecifieke, sectorale en regionale cyberinitiatieven. In de loop van de tijd zijn er verschillende diensten ontwikkeld om ondernemend Nederland verder te helpen. De Basisscan Cyberweerbaarheid² is een *self-assessment* om vast te stellen waar een bedrijf staat ten opzichte van de vijf basisprincipes. De Risicoklassenindeling Digitale Veiligheid³ geeft in elf vragen inzicht in welke digitale risico's een bedrijf loopt op basis van het bedrijfsprofiel. Ook op het gebied van procesautomatisering is er een *tool* ontwikkeld om ondernemers te

¹ Kamerstuk 2643-465.

² <https://basisscan.digitaltrustcenter.nl/>.

³ <https://www.digitaltrustcenter.nl/risicoklasse>.

'WAT DOE JE ALS JE GETROFFEN WORDT DOOR EEN DIGITAAL INCIDENT?'

laten zien wat ze kunnen verbeteren op het gebied van hun *Operational Technology* (OT). Deze *tools* zijn gratis en beogen het bewustzijn van ondernemers te vergroten en hen aan te zetten tot hen nemen van noodzakelijke maatregelen.

Naast de *tools* heeft het DTC ook informatieproducten. Een voorbeeld hiervan is het Calamiteitenplan. Centrale vraag die daarmee wordt beantwoord is: wat doe je als je getroffen wordt door een digitaal incident? Ook zitten er praktische tips in: wie bel je bij een incident en heb je die telefoonnummers paraat? Het DTC maakt niet alleen eigen producten, maar draagt ook bij aan producten van anderen. Een goed voorbeeld is het recent herziene *Cybersecurity Woordenboek* van de CSA⁴. Met dit woordenboek in de hand wordt de ondernemer concreet geholpen de materie te begrijpen.

Ondernemers helpen ondernemers

Met ondernemersverhalen worden concrete casussen en tips van getroffen bedrijven verteld. Dit zorgt voor herkenning en meer bewustwording bij de doelgroep: dit kan mij ook overkomen. Het DTC heeft daarom ook een online platform gemaakt waar ondernemers met elkaar ervaringen en informatie kunnen delen. Deze DTC Community is bovendien een belangrijk instrument om urgente cyberdreigingen snel bekend te maken bij de ondernemersdoelgroep en IT-dienstverleners.

Sinds juni 2021 verstrekt het DTC ook rechtstreeks informatie aan individuele ondernemers over bij de overheid bekende kwetsbaarheden in de netwerk- en informatiesystemen van

bedrijven. Met deze waarschuwingen kunnen bedrijven direct maatregelen (laten) treffen om cyberaanvallen of -incidenten te voorkomen of beperken.

Succesfactoren

Een belangrijke succesfactor van het DTC is de samenwerking met andere overheidsorganisaties als het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), maar ook de samenwerking met andere departementen. Daarnaast zijn het de mensen die een organisatie maken. Het DTC heeft daarom een divers maar gebalanceerd team samengesteld. Dit team, bestaande uit specialisten op het gebied van communicatie en (online) promotie, relatiemanagers en cybersecurityadviseurs en ambtelijke ondersteuning, zoekt zo veel mogelijk aansluiting bij ondernemers.

Omdat bijna alle medewerkers ook uit het bedrijfsleven komen, kan de verbinding met ondernemers makkelijker worden gelegd. Daarnaast is de compactheid van het team een groot voordeel. Lijntjes zijn kort, de richting is duidelijk en samen wordt gewerkt aan een doel.

Toekomst

Er zijn lichtpunten te zien. Meer bedrijven zijn zich in toenemende mate bewust van het feit dat ze actie moeten ondernemen en weten het DTC en de informatie te vinden. Een belangrijk aandachtspunt blijft het probleem van ransomware. Maar ook de toenemende afhankelijkheid van de digitale processen en diensten en de verdere vervlechting van systemen en netwerken maken dat ondernemers in actie moeten komen. Het DTC ziet

'EEN BELANGRIJK AANDACHTSPUNT BLIJFT HET PROBLEEM VAN RANSOMWARE'

Basisprincipes van digitaal weerbaar ondernemen

1. Inventariseer kwetsbaarheden

Inventariseer de ict-onderdelen, kwetsbaarheden en maak een risico-analyse. Bij risico's kijk je naar beschikbaarheid, integriteit en vertrouwelijkheid.

2. Kies veilige instellingen

Controleer de instellingen van apparatuur, software en netwerk- en internetverbindingen. Pas standaardinstellingen aan en kijk kritisch naar functies en diensten die automatisch "aan" staan.

3. Voer updates uit

Controleer of apparaten en software up-to-date zijn. Installeer beveiligingsupdates direct. Schakel automatische updates in zodat je apparaten en software voortaan altijd draaien op de laatste versie.

4. Beperk toegang

Definieer per medewerker tot welke systemen en data toegang vereist is om te kunnen werken. Zorg dat toegangsrechten worden aangepast als iemand een nieuwe functie krijgt of bij de onderneming vertrekt.

5. Voorkom virussen en andere malware

Er zijn vier manieren om malware te voorkomen: stimuleer veilig gedrag van medewerkers, gebruik een anti-virusprogramma, download apps veilig en beperk de installatiemogelijkheden van software.

in samenwerking de sleutel om samen met bedrijven, IT-dienstverleners en hele bedrijfsketens, de weerbaarheid te vergroten. Per slot van rekening heeft een verstoring bij een bedrijf allang niet meer alleen gevolgen voor dat individuele bedrijf: hele ketens van bedrijven hebben daar last van.

Meer informatie over het verbeteren van de weerbaarheid van bedrijven en het werk van het Digital Trust Center? Kijk op www.digitaltrustcenter.nl.

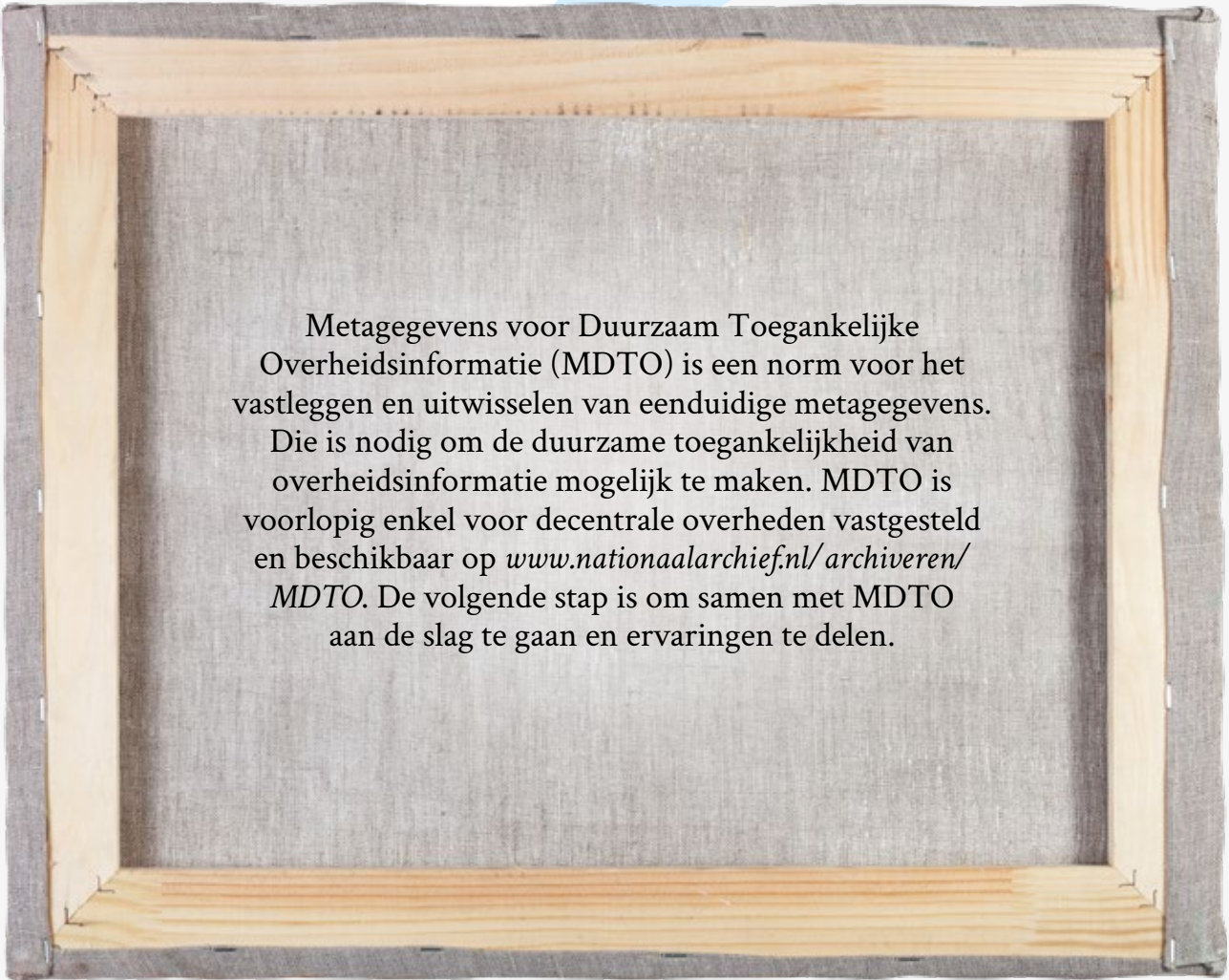
⁴ <https://www.cybersecurityalliantie.nl/producten-tools/cybersecurity-woordenboek/>.

Tekst **Simone Driessen**

Simone Driessen is webredacteur
bij het Nationaal Archief

Samen van theorie naar praktijk

Op kop met MDTO



Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie (MDTO) is een norm voor het vastleggen en uitwisselen van eenduidige metagegevens. Die is nodig om de duurzame toegankelijkheid van overheidsinformatie mogelijk te maken. MDTO is voorlopig enkel voor decentrale overheden vastgesteld en beschikbaar op www.nationaalarchief.nl/archiveren/MDTO. De volgende stap is om samen met MDTO aan de slag te gaan en ervaringen te delen.

'MET GROTE EN KLEINE PRAKTIJKERVARINGEN ONTWIKKELT DE MDTO-COMMUNITY ZICH VERDER'

Om organisaties te ondersteunen bij het toepassen van MDTO startte het Nationaal Archief in het najaar van 2021 met een koplopersgroep. Vier archiefinstellingen met archiefvormers, twee gemeenten, een waterschap en een uitvoeringsorganisatie hebben elkaar in vier sessies vraagstukken voorgelegd. 'Dat organisaties zich hiervoor aanmelden kwam echt voort uit een kennisbehoefte,' vertelt implementatiemanager kennisproducten Corinne Boeijinga van het Nationaal Archief. 'Metadatering is geen gemakkelijk onderwerp. Afgeronde praktijkvoorbeelden met MDTO bestaan nog niet. Samen interpretatievraagstukken bespreken en zoeken naar oplossingen werkt motiverend en biedt inzichten en vertrouwen. De toepassing van MDTO is overigens ook voor het Nationaal Archief nog een leerproces: we moeten MDTO zelf nog implementeren. Al beschikken we als ontwikkelaar van MDTO over veel kennis. Het is een model, die elke organisatie op de eigen situatie zal toepassen.'

Specifiek

Dat vertalen naar de eigen situatie is soms best een uitdaging. De toepassing van MDTO in een zaakstelsel is hier een voorbeeld van. Deze systemen bevatten vaak velden die niet direct in MDTO terugkomen. Door hier samen over te praten kom je tot oplossingen voor dit soort specifieke gevallen.

Alex l'Ami, adviseur informatiebeheer bij het ministerie van Defensie heeft vergelijkbare ervaringen met de vertaalslag binnen zijn context. Als een van de eersten binnen de rijksoverheid zijn zijn collega's en hij in hun organisatie aan de slag gegaan met MDTO. Zij hebben

op basis van MDTO een metadataschema met eigen begrippenlijsten ontwikkeld. Niet alle attributen zijn hetzelfde als in MDTO, maar zijn hier wel naar te vertalen. Zo hebben zij het attribuut "beperking gebruik" vertaald naar "rubricering en merking". Generieke voorbeelden die in MDTO worden genoemd zijn vervangen door specifieke voorbeelden voor Defensie, zodat de gebruikers in de organisatie de bedoeling begrijpen.

Op termijn gaan ze de inrichting van een aantal informatiesystemen baseren op hun eigen schema en daarmee ook op MDTO. De scope blijft beperkt tot de systemen waar informatie zit die aan het Nationaal Archief wordt overgedragen.

Online spreekuur

In aanvulling op deelname aan de koplopersgroep kunnen organisaties hun eigen vraagstukken over MDTO voorleggen in een online spreekuur. 'Ik ben nog zoekende in hoe we MDTO goed kunnen toepassen in onze organisatie. Daarom is het fijn dat het Nationaal Archief een speciaal spreekuur heeft opgezet. Zo kun je op een laagdrempelige manier vragen stellen aan de experts,' vertelt deelnemer Karin Tiel van BAR, de uitvoeringsorganisatie van de gemeenten Barendrecht, Albrandswaard en Ridderkerk. De spreekuren staan aangekondigd in de agenda op [Kia.pleio.nl](https://kia.pleio.nl). Iedereen kan hier aan deelnemen.

Het begin van een *community of practice* is ontstaan. De eerste gebruikers zijn bezig met de toepassing van MDTO. Zij hebben *mappings* gedaan, interpretatievraagstukken behandeld, organisatiespecifieke begrippenlijsten bedacht, modellen gebouwd en redactionele onduidelijkheden opgehelderd. In de koplopersgroep zijn die ervaringen uitgewisseld. Deze organisaties gaan hun kennis verder uitdragen en delen met anderen.

Met alle grote en kleine praktijkervaringen ontwikkelt en verbetert de community van MDTO verder. MDTO is namelijk niet van het Nationaal Archief maar van en voor de gebruikers.

Tekst **Chantal Menting**Chantal Menting is plaatsvervangend
gemeentearchivaris van de gemeente AmersfoortSamenwerkende toezichthouders
in Amersfoort

Schotloos toezicht

De wereld van informatie groeit steeds groter en sneller. Hoe bewaar je informatie op de juiste wijze en hoe beveilig je die? En hoe zorg je ervoor dat informatie en persoonsgegevens niet zomaar op straat komen te liggen? In Amersfoort werken toezichthouders daartoe steeds intensiever samen.



Het interne toezicht in de gemeente kent vier zogenoemde interne toezichthouders: de *concern controller*, de functionaris gegevensbescherming (FG), de gemeentearchivaris en de *chief information security officer* (CISO). De onderwerpen waarmee deze interne toezichthouders zich bezighouden, kennen overlap en/of veel raakvlakken. In 2018 is de gemeente daarom gestart met reguliere overleggen om overkoepelende risico's en aandachtspunten binnen de organisatie te signaleren.

Toezichthoudende functie: Vierhoeksoverleg

In 2020 hebben deze reguliere overleggen meer vorm gekregen in een zogenaamd Vierhoeksoverleg. De aanleiding om deze samenwerking te intensiveren is dat er

in de snel veranderende informatiewereld geen schotten te plaatsen zijn tussen de verschillende disciplines. Het ontstaan van verbonden partijen (doordat lokale overheden met elkaar samenwerken of bepaalde taken door een externe, verzelfstandigde organisatie laten uitvoeren, red), met name in het sociaal domein, zorgt ervoor dat je te allen tijden informatie moet beveiligen, zodat persoonsgegevens niet op straat komen te liggen. Maar het gevolg is ook dat je te allen tijden bij die informatie moet kunnen. Dat kan soms tegenstrijdige belangen met zich mee brengen, omdat wet- en regelgeving op dat terrein niet consistent is. Daarom is het goed om met de verschillende toezichthouders regelmatig te overleggen over dit soort zaken: aan de voorkant alle aspecten meenemen en proberen te tackelen.

'HET VIERHOEKSOVERLEG KOMT TENMINSTE MAANDELIJKS BIJ ELKAAR'

Het Vierhoeksoverleg komt tenminste maandelijks bij elkaar. Dit kan ook vaker zijn als er zaken spelen die kortcyclisch afstemming behoeven. Ook als er vanuit de organisatie of vanuit de toezichthouders behoefte is om over een bepaald onderwerp door te praten, zoals de Wet open overheid (Woo) of over architectuur binnen de gemeente, dan wordt een aparte sessie ingepland om elkaar bij te praten.

Het doel van dit overleg is om de samenwerking, effectiviteit en kwaliteit van het intern toezicht te ontwikkelen en bevorderen op zowel strategisch, tactisch als operationeel niveau. Dit betekent dat onder meer het onderstaande hierin plaatsvindt:

- Elkaar informeren over zaken die in relatie tot de verschillende toezichtdisciplines spelen. Hierbij bekijken waar overlap zit en samenwerking meerwaarde heeft of zelfs noodzakelijk is.
- Signaleren van knelpunten in toezichtrelevante kwesties binnen de organisatie.
- Beeld vormen over de mate waarin de organisatie zich doorontwikkelt en of er sprake is van voldoende opvolging van aanbevelingen vanuit de toezichthouders.
- Afstemmen opzet, *tone of voice*, timing, samenhang en inhoud van toezichtrapportages.
- Beoordelen impact nieuwe regelgeving op toezicht, zoals Archiefwet, BIO, Woo, Wpg, etcetera.
- Bespreken doorontwikkeling rollen en functie toezichthouders binnen de organisatie. Zoals bijvoorbeeld richting (de vorming van) de CIO office.
- Beoordelen of *checks and balances* binnen de organisatie voldoende zijn vanuit toezichthoudend perspectief.

De besprekingen vinden plaats op basis van een agenda. Van de bespreking wordt een kort verslag gemaakt. Hierbij worden werkafspraken en actiepunten vastgelegd. Het verslag wordt ter kennisgeving in de directie gebracht.

Verder functioneert het Vierhoeksoverleg als een intervisiegroep: dilemma's, vraagstukken en knelpunten vanuit de functie-uitoefeningen komen binnen een informele en vertrouwelijke setting op tafel en dat draagt bij aan de ontwikkeling van de mens als toezichthouder.

Adviserende functie: CIO office

Naast een toezichthoudende functie hebben de interne toezichthouders van de gemeente Amersfoort ook een adviserende functie. Vanuit deze rol hebben drie toezichthouders - FG, CISO en gemeentearchivaris - zitting in het CIO office. De *concern controller* sluit hierbij af en toe aan, wanneer dit gewenst is.

In Amersfoort is in 2021 het CIO office van start gegaan. In 2019 en 2020 is de noodzaak van een CIO office in verschillende audits en toezichtverslagen aan de orde gekomen. Er zijn verschillende overlegvormen: 1 keer in de 6 weken zit de CIO samen met de portfoliomanager en de toezichthouders om tafel om overkoepelende onderwerpen te bespreken. Eens in de 2 maanden sluiten de toezichthouders aan bij het CIO office-overleg waarin de adviseurs op het gebied van informatievoorziening zitting hebben om strategische thema's uit te werken. In dit overleg proberen we als toezichthouders aan de voorkant te adviseren over de thema's en de bandbreedte van de kaders en wet- en regelgeving waarmee we te maken hebben.

Samenwerking intensiveren

Zoals gezegd, is de samenwerking tussen de interne toezichthouders de afgelopen 2 jaar enorm versterkt. Maar we zijn er nog niet. Op dit moment hebben we in onze vakgebieden wel overkoepelende thema's benoemd waar we risico's zien, zoals verbonden partijen, of waar we raakvlakken zien, zoals privacy, security en *archiving by design*. Op deze onderwerpen willen we het komend jaar nog meer samenwerking zoeken.

Een tweede aspect waar we komend jaar naar gaan kijken is in hoeverre onze verschillende jaar- of toezichtverslagen nog meer in samenhang richting de organisatie, de directie, het college en de raad gebracht kunnen worden. Een eerste stap zetten we dit jaar door rond hetzelfde tijdstip onze rapportage op te stellen en vast te laten stellen. Aanbieden aan directie en college zal gebeuren door middel van een oplegnotitie waarin we overkoepelende actiepunten benoemen. Voor 2023 is het onze ambitie om tot een rapportage te komen. Of dit haalbaar is, moet komend jaar uitwijzen, maar gezien de problematiek rondom de drie vakgebieden *privacy*, *security* en *archiving* is dit wel wenselijk.

'DE INTERNE TOEZICHTHOUDERS VAN DE GEMEENTE HEBBEN OOK EEN ADVISERENDE FUNCTIE'

Tekst **Walter van Wijk**

Walter van Wijk is coördinator van de privacy community van CIP

Terugblik

Week van de Privacy

Hoe leeft de politie de privacywetgeving na en hoe houdt de functionaris gegevensbescherming daarop toezicht? Is de politie ook je beste (privacy)vriend? En wist je dat er voor bepaalde beroepsgroepen volledig geautomatiseerde HRM-toepassingen zijn ontwikkeld voor werving en selectie?

Over deze en andere actuele thema's en onderwerpen op het gebied van privacy organiseerde het Centrum Informatiebeveiliging en Privacybescherming (CIP) onlangs een serie webinars tijdens de jaarlijkse Week van de Privacy.

De webinars werden georganiseerd in samenwerking met de Autoriteit Persoonsgegevens (AP). Alle vijf kunnen worden teruggekeken, maar ook als podcast beluisterd.

Op weg van onbewust onbekwaam naar onbewust bekwaam

Webinar 1: Henri Raaphorst (audit beroepsorganisatie Norea) en Arjan Kapteijn (AP) vertellen over de verplichte Wpg-audit (Wet politiegegevens) voor organisaties met boa's. Deze bijzondere opsporingsambtenaren hebben kennis nodig van de AVG en de Wpg.

Daarop wordt nu toezicht gehouden vanuit de AP. De deadline voor het indienen van het eerste Wpg-auditrapport is inmiddels verschoven naar 31 december 2022, maar er is voor veel organisaties wel echt werk aan de winkel. Verantwoordelijken wordt geadviseerd om met de diverse soorten betrokkenen in gesprek te gaan en de processen te leren kennen. Om op weg te gaan van onbewust onbekwaam naar onbewust bekwaam. Ook het aantal auditors is (nog) beperkt, dus wacht niet te lang om de weg naar het voldoen aan deze nieuwe verplichting in te slaan.

Is de politie ook je beste (privacy) vriend?

Webinar 2: Hoe ontwikkelt het naleven van de privacywetgeving zich binnen de politie en hoe houdt de functionaris gegevensbescherming (FG) daarop toezicht? Ben van Hoek, FG bij de politie, en Merel Koning, senior beleidsmaker bij Amnesty, stellen deze vragen en onderzoeken ook het spanningsveld tussen privacy en opsporing. Inmiddels wordt door de politie flink geïnvesteerd in de privacy-organisatie en -aanpak en maakt de korpsleiding chefsache van het onderwerp. Amnesty is waakzaam en kritisch,

en deelt hun visie en opmerkingen daarover. Naast de politie heeft zij ook gemeenten nadrukkelijk op hun netvlies, bijvoorbeeld op het gebied van verantwoorde opsporing van bijstandsfraude.

Positionering Functionaris Gegevensbescherming

Webinar 3: We bespreken de recent gepubliceerde *position paper* van de AP: wat is belangrijk voor het goed functioneren van een Functionaris Gegevensbescherming? Het AP ziet de FG als adviseur, toezichthouder, informatieknooppunt en onderzoeker. Maar er is ook aandacht voor escalatie bij klachten, en toegang tot bestuurders. Hoe is die lijst met uitgangspunten ontvangen door gemeenten? Hier is recentelijk onderzoek naar gedaan door de VNG, want die wil de rol van de gemeentelijke FG's versterken. Het onderzoek toont onder meer aan dat er veel deeltijd-FG's (veelal met juridische achtergrond) in gemeenteland zijn, en er heerst een breed ervaren gevoel van gebrek aan voldoende tijd voor het adequaat uitoefenen van de functie. Met als sprekers van Marjolein Louwerse (AP) en David van den Berg (VNG).

Over Bartje en bruine bonen

Webinar 4: Privacy = Governance! Welke besturingsmechanismen hanteren ministeries en wat is de visie daarop vanuit KPMG? Hoe organiseer je dit op de werkvloer? Onder meer door bestuurders goed op de hoogte te houden met behulp van een ambtelijk dashboard. Daarmee worden de hoofdlijnen en

'CIP ONDERSTEUNT DE NEDERLANDSE OVERHEID OM INFORMATIEVEILIGHEID OP PEIL TE KRIJGEN'

Over CIP

Het Centrum Informatiebeveiliging en Privacybescherming is in 2012 opgericht en ondersteunt de Nederlandse overheid om informatieveiligheid op peil krijgen en te houden. CIP doet dat door het ontwikkelen en delen van kennis op het gebied van onder andere privacybescherming, data-ethiek, cyber security, secure software development, IoT en AI. Aanvullend ontwikkelt CIP ondersteunende instrumenten, zoals *self-assessments*, handreikingen, volwassenheidsmodellen, serious games, en dergelijke. Daarnaast stimuleert en ondersteunt CIP namens het ministerie van BZK de toepassing van de Baseline Informatiebeveiliging Overheid (BIO) en de ICO-Wizard (Inkoopeisen Cybersecurity Overheid). In die laatste zijn onlangs ook *privacy by design*-maatregelen opgenomen.

Alle producten en diensten van CIP zijn kosteloos toegankelijk. Meer informatie is te vinden op de site: www.cip-overheid.nl.

kritische ontwikkelingen een aantal keer per jaar inzichtelijk gemaakt en toegelicht. Verder is er een nadrukkelijk pleidooi om zelf je belangen (en het daarvoor benodigde budget) te claimen en te verdedigen (Bartje en bruine bonen!). En dat in een realistische bestuurdersbeleving met tal van andere belangen en prioriteiten, waarbij de primaire bedrijfsprocessen vaak prevaleren. Vanuit hun ervaring spreken Pieter de Groot (ministerie van Justitie en Veiligheid) en Laura Huijts (KPMG) hierover.

AI en mensenrechten

Webinar 5: Over AI en mensenrechten. In het nog jonge werkveld van kunstmatige intelligentie (AI), algoritmes en *machine learning* moeten - naast informatieveiligheid en privacy - ook de mensenrechten worden bewaakt. Welke criteria worden daarbij aangehouden en wat wordt er al toegepast? Gerald Hopster van de AP licht de focus van het Agentschap toe, namelijk door AI-toepassingen te bekijken vanuit de AVG-principes: rechtmatig, behoorlijk en transparant. En hoe zit het met betrokkenheid van burgers, discriminatie en gelijke behandeling (verwoord door Quirine Eijkman, vanuit het College voor de Rechten van de Mens)? Onder meer AI-toepassingen voor HRM-selectie en kappers passeren de revue.

De webinars en andere interessante video's over informatiebeveiliging en privacybescherming zijn ook terug te vinden op het CIP YouTube-kanaal. Podcasts kun je beluisteren via je eigen favoriete app of het CIP Podcast platform.

WAAROM OPEN SOURCE GOED BIJ DE OVERHEID PAST

Bij de publieke zaak passen openheid en transparantie, en dus ook open source software. Veiligheid? Moet je absoluut serieus nemen, maar open is iets anders dan onveilig, zegt Koos Steenbergen, beleidsadviseur open source bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 'Onze wetgeving komt in openheid tot stand, dat mag je dan ook van de systemen voor controle en uitvoering verwachten.'



Begin februari is de Massive Open Online Course (MOOC) *Open source: van ambitie naar realiteit* gestart. Deze MOOC bestaat uit vier inzichten (filmpjes) plus tools en praktijkverhalen, die vooral zijn bedoeld om mensen aan het denken te zetten. 'De doelgroep is heel breed,' legt Koos Steenbergen, projectleider bij het ministerie van BZK, uit. 'We richten ons op overheidsprofessionals die werkzaam zijn bij het rijk, de provincie of gemeenten. Dat kunnen bestuurders of adviseurs zijn, die met software te maken hebben. We willen hen bewust maken van de mogelijkheden van open source.'

Identieke systemen

Open source software wordt ook buiten de overheid veel gebruikt, in het bedrijfsleven bijvoorbeeld. Steenbergen: 'Het is efficiënt, want je kunt oplossingen die ontwikkeld zijn, en dus de kennis en ervaring die daarbij horen, hergebruiken. Voor de verschillende overheden in Nederland zijn veel identieke systemen nodig; het ligt voor

'OPENHEID IS IETS ANDERS DAN ONVEILIGHEID'

de hand om die dan maar een keer te ontwikkelen of in te kopen en te delen.' Naast efficiënt omgaan met publieke middelen zit daar ook een meer fundamentele kant aan, benadrukt Steenbergen. 'Openheid en transparantie passen bij de rol van de overheid. We werken steeds meer digitaal, maken steeds vaker gebruik van kunstmatige intelligentie en algoritmen, onder meer voor systemen die inwoners controleren. Onze wetgeving komt in openheid tot stand, dat mag je dan ook van de systemen voor controle en uitvoering verwachten. We moeten vaker nadenken over vragen als: gaan we software open (mede) ontwikkelen of inkopen, wanneer is dat wel mogelijk en wanneer niet?'

Veiligheid

Steenbergen beseft terdege dat er dis-

cussiepunten rond open source software zijn, bijvoorbeeld als het om veiligheid gaat. 'Maar openheid is iets anders dan onveiligheid. Je kunt heel goed open laten zien dat je systemen uitstekend beveiligd zijn, zonder dat je iedereen zo maar de sleutels geeft. En hoe veilig zijn systemen, waarvan je niet weet hoe ze ontwikkeld zijn? Er zullen altijd mensen zijn die ze toch proberen te kraken en als je niet weet hoe die systemen ontwikkeld zijn, moet je maar vertrouwen op de leverancier. Ook word je dan afhankelijker van die partij.'

'De MOOC gaat maar deels over de technische kant en is vooral bedoeld om mensen te laten zien waarom open (source) ontwikkelen zo goed bij de overheid past. Dan gaat het over de waarden van overheidsprofessionals bijvoorbeeld. Ook gaan de inzichten in op de praktijk, zoals de CoronaMelder-app, en discussiepunten. En wat we er in de toekomst zoal mee kunnen.'

De MOOC *Open source: van ambitie naar realiteit* kan bekeken worden op <https://omooc.nl/moocs/open-source/>.

‘Stap uit je comfortzone’

Organisatie: Doc-Direkt
Begonnen in: december 2021
Functie: I-adviseur

Het vakgebied informatiebeheer kent een grote diversiteit aan collega's. Waar de een al decennialang actief is, komt de ander net kijken. In deze rubriek maken we kennis met de nieuwelingen. In deze aflevering is het woord aan Anniek van der Pijl.

Hoe ben je in deze functie terechtgekomen?

‘Ik kom oorspronkelijk vanuit de psychologie en ben ook werkzaam geweest binnen de GGZ. Een tijd geleden was ik toe aan verandering. Ik zocht een baan waarin leren mogelijk was, waarin mijn kwaliteiten naar voren kwamen en waarin de mogelijkheid bestond kennis te maken met informatie en data. Niet geheel onbelangrijk: ik wilde wel in de publieke sector werken. Ik ben vervolgens begonnen met een *traineeship* informatiemanagement (bij Modis) en kwam uiteindelijk bij Doc-Direkt terecht.’

‘De twee vakgebieden lijken ver uit elkaar te liggen, maar ik denk dat mijn achtergrond goed kan helpen. Er zijn zeker overeenkomsten. Zo is communicatie ook als I-adviseur heel belangrijk. En dan vooral het doorvragen, niet altijd direct het eerste antwoord accepteren. Goed kijken of we elkaar echt begrijpen of alles echt duidelijk is.’

‘Wat ik denk leuk te gaan vinden, is de diversiteit aan werkzaamheden. Ook voelt het goed om een bijdrage aan de overheid te mogen leveren op het gebied van informatiebeheer. Dat merkte ik al bij een opdracht die we nu nog aan het uitvoeren zijn. Dat gaat over een parlementaire enquête. De opdracht heeft geholpen bij het begrijpen wat een parlementaire enquête is, het belang van zo'n enquête, hoe wetten hierbij een rol spelen, wat de connectie is met informatiehuishouding en welke rol je zelf daarin kunt gaan spelen.’

Hoe ga je je kennis op peil houden en heb je al verbetervoorstellen gedaan?

‘Ik zit nu nog in de introductiefase en daarin zijn we al volop aan het leren. Maar het stopt hierna natuurlijk niet. Na de inwerkperiode zal ik mezelf allereerst afvragen wat ik nodig denk te hebben om mijn werkzaamheden volledig en prettig uit te kunnen voeren. Vervolgens ga ik kijken

waar mijn kwaliteiten en leerpunten liggen. Het op peil houden van kennis en vaardigheden kan verschillende vormen aannemen. Door middel van opleidingen en cursussen kan ik mijn kennis verrijken.’

‘In mijn werk bestaat een prettige openheid dus ik voel mij vrij om vragen te stellen aan collega's. Meelopen met hen geeft ook inzicht waar soms nog wat bij te spijkeren valt of waar ik graag nog meer van wil leren. Tot slot blijft de grootste uitdaging je valkuilen herkennen en daaraan werken. Daar moet je soms voor *out of the box* denken en uit je comfortzone stappen. Ook mijn kritische blik speelt daarbij een belangrijke rol, later zal ik zeker kijken naar verbeterpunten, maar ik kan met de kennis en *feeling* die ik tot nu met het vak heb nog geen uitspraak doen over een verbetervoorstel.’

Heb je advies voor iemand die ook aan de slag wil als informatiebeheerder?

‘Het is eerder een algemeen advies dan specifiek gericht op informatiebeheer. Ik heb geleerd dat mogelijkheden echt bestaan. Weet waar je kwaliteiten en energiegevers liggen. In mijn geval kwam ik erachter dat informatiebeheer minder stoffig is dan het soms klinkt en dat er een wereld voor je opengaat binnen dit vakgebied.’

Bij de les blijven

Het volgende nummer van ons blad zal in het teken staan van Artificial Intelligence (AI) oftewel kunstmatige intelligentie. Is deze technologie de opmaat voor nieuwe kansen binnen ons vakgebied of is het echt de doodsteek? Het moge duidelijk zijn dat de AI en mogelijkheden die AI biedt eindeloos zijn en dat we nog maar aan de vooravond staan van wat we de vierde fase van de industriële revolutie zijn gaan noemen. Het beeld van de experts is dat AI onder de streep voor meer banen gaat zorgen maar dat deze banengroei niet geldt voor de laaggeschoolden. Zij oefenen beroepen uit

waarin AI een rol kan spelen. Wat opvalt is het gemak waarmee AI aan ons wordt verkocht. Bijvoorbeeld met het argument dat het de wereld een mooiere plek maakt. Maar de werkelijkheid is anders. Hoewel het schrijven van een algoritme in de basis niet moeilijk lijkt te zijn met behulp van programmeertalen als Python en R, zal AI voor de meesten voorlopig een ver-van-mijn-bedshow blijven. Dus moet je er als burger maar op vertrouwen dat organisaties en overheden die met AI werken hun zaken goed op orde hebben en het beste

met jou als burger voorhebben. *Bottomline* is dat we algoritmes steeds grotere beslissingen laten nemen met steeds grotere risico's van dien. We mogen dan ook blij zijn dat we in een land leven waar terecht ook de ethische kant van het gebruik van AI aandacht krijgt. Maar in een digitale wereld waar traditionele grenzen steeds meer vervagen, blijft het zaak voor informatieprofessionals om bij de les te blijven en ons allen te behoeden voor bedoeld en onbedoeld misbruik van AI.

Edwin Driessen is redactielid Od

SERVICEBERICHT

Modernisering van de Archiefwet

Dat de huidige Archiefwet is verouderd en minder goed toe te passen op digitale informatie is een open deur. Op het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) wordt daarom al enkele jaren hard gewerkt aan de modernisering van de wet. Helaas kan ex-minister Arie Slob zijn wetsvoorstel niet meer in de Tweede Kamer verdedigen. Die uitdaging

ligt nu op het bordje van de nieuwe staatssecretaris van OCW, Gunay Uslu. Aan de behandeling in de Kamer gaat overigens op 23 februari een rondetafelgesprek vooraf, waarin Kamerleden zich door verschillende experts laten informeren.

Kennisdossier op KIA

Op de homepage van KIA staat in het blok Campagnes een knop waarmee je direct kunt navigeren naar het kennisdossier Modernisering Archiefwet. In dit kennisdossier is actuele informatie te vinden over

de nieuwe Archiefwet. Natuurlijk vind je er de tekst van de wet zoals deze bij de Tweede Kamer is ingediend. Je vindt er ook informatie over het voortraject, over verschillende verwante kennisproducten en een rubriek met doorverwijzingen naar relevante andere websites.

Veelgestelde vragen

In de rubriek Veelgestelde vragen vind je ten slotte een toelichting op de meest in het oog springende wijzigingen in de wet. Met specifieke vragen kun je ook

terecht bij het projectteam van het ministerie van OCW, via archiefwet@minocw.nl. Over de definitieve redactie van de Archiefregeling en het Archiefbesluit kun je overigens nog meepraten. Zie daarvoor onder Klankbordgroepen de nog openstaande mogelijkheden. En straks volgt natuurlijk de internetconsultatie over ABAR, zoals het besluit en de regeling in het jargon meestal worden aangeduid.

Wil je meediscussieren over dit onderwerp? Ga dan naar het KIA-Kennisplatform Informatierecht.

Kennissnetwerk
Informatie en Archief

Begrip in plaats van grip

Hoe complex is je opgave?

Hoe kunnen we de complexiteit waarin we informatie- en archiefbeheer als taak gepositioneerd zien met meer succes te lijf gaan? Met begrip in plaats van grip, aldus Herrie Geuzendam en Angela Riddering in - de titel zegt het al - *BEgrip; werken met complexiteit voor de publieke professional*.



Het Nationaal Archief heeft eerder rondom *archive by design* presentaties gehouden waarin de ontwikkeling van informatiebeheer wordt omschreven als die van de postkoets naar de auto. In de kern gaat die vergelijking nog steeds op, en gaat gepaard met vele veranderingen aan de koets zelf en de infrastructuur waarop we ons inmiddels met elektrische auto's op asfaltwegen voortbewegen, inclusief verkeerslichten en rotondes, et cetera. Een transitie die we doormaken met het informatie- en archiefbeheer is dat we meer onderkennen dat relevante informatie rondgaat in de taaksystemen, kantoorautomatisering, sociale media en samenwerkingsruimten. We ervaren het beheren van die informatie als complex en het Nationaal Archief noemde die opgave al eerder een *wicked problem*: een taai vraagstuk dat moeilijk oplosbaar is. Zo'n vraagstuk laat zich slecht structureren en beheersen. Niemand weet precies hoe de vork in de steel zit. Woorden die ermee samenhangen zijn: ongestructureerd, ontembaar en duivels.

Stappen

En nu: hoe kun je dit boek lezen en complexiteit met meer succes te lijf gaan? Daarbij is het belangrijk om na te denken over:

1. Hoe complex is je opgave?
2. Wat heeft je organisatie nodig om met complexiteit om te gaan?

3. Hoe ga je om met bestuurlijke advisering bij complexe vraagstukken?
4. Wat vraagt complexiteit van jou als persoon?
5. Hoe maakt jouw organisatie impact op compacte opgaven?

Je kunt het boek lezen, erin grasduinen of het slothoofdstuk lezen, want daarin komt aan de orde hoe om te gaan met onvoorspelbaarheid, want daar hebben we veel behoefte aan. Zoveel behoefte, is mijn indruk, dat we - ook als het niet werkt - vasthouden aan werkwijzen die ons niet helpen. Ik raad je aan het framework voor begrip dat de auteurs ontwikkelen op te stellen. Door dit framework te doorlopen breng je in beeld welke stappen publieke professionals (jij en je collega's van de taakuitvoering) doorlopen om grip op informatie te krijgen en welke knooppunten er ontstaan. Per knooppunt worden rollen geschetst die jij en je collega's kunnen vervullen om de opgave succesvol te maken.

Hulplijnen

Als je het boek heb doorgewerkt dan kom je tot een aantal inzichten:

1. Om grip op informatie te krijgen is het een belangrijke stap om begrip te hebben van de complexiteit waar informatie zich bevindt, binnen en wellicht buiten de organisatie.

2. Heb je te maken met een complex vraagstuk, of is het gewoon (slechts) ingewikkeld?
3. De informatieprofessional maakt het verschil binnen de organisatie, dat effect is het grootst als je durft om je persoonlijk te ontwikkelen of je te laten bijstaan door mensen binnen of buiten je organisatie die je kunnen helpen.
4. Dit pleit voor een assertieve reflectie, voor een progressieve luisterhouding, voor radicale tijdelijkheid en voor verdragend optreden, aldus Jan van Ginkel, concerndirecteur Zuid-Holland en één van de publieke professionals die het boek aanbeveelt.

Het boek sluit af met interviews en hulplijnen. Meerdere publieke professionals en wetenschappers vertellen waarvoor zij zich gesteld zagen, hoe daarmee werd omgegaan en wat anderen van hun aanpak kunnen leren. De hulplijnen variëren van checklists tot vindplaatsen en bieden handvatten om daadwerkelijk aan de slag te gaan. Denk bij hulplijnen aan waardevol onderzoek, datagedreven innoveren, bouwen aan vertrouwen, oefeningen in openheid of ben ik een goede bestuurlijk adviseur.

Van harte aanbevolen.

Herrie Geuzendam en Angela Riddering, *BEgrip; werken met complexiteit voor de publieke professional*. Boom, 2021.

Tekst **Eric Kokke**

Eric Kokke is redactielid Od

Toekomst van de archieffunctie

Eind november verzorgde het Future Lab-project van Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI) en de KNVI onder begeleiding van Reframing Studio een werkatelier. In dat atelier dachten de deelnemers niet alleen na over de toekomst van de archieffunctie, maar probeerden ze die ook te concretiseren. Dit werkatelier sluit daarmee aan bij eerdere verkenningen die de KNVI in opdracht van het Kennisplatform Informatie en Archief (KIA) heeft gedaan.

Om de deelnemers in de juiste *mindset* te krijgen verzorgde Roland Bisscheroux (directeur-archivaris bij Waterlands Archief) een korte introductie over de noodzaak van innovatie in het archief. Gevolgd door een mini-college van Future Lab over de methodiek die heeft geleid tot het rapport *De informatiehuishouding van het rijk 2030* (Bit.ly/3GzsN-DU). Beide presentaties waren een opmaat om in drie deelsessies aan de slag te gaan met de toekomst van de archieffunctie.

DEELSESSIE 1

Beleidsvernetwerking – conceptueel vooruitkijken

Context van de ontwerpvisie

Bij de overheid wordt nog vaak onafhankelijk van elkaar gewerkt, terwijl we onze inzet juist moeten samenbrengen om aan maatschappelijke opgaves te werken. We zijn immers een maatschappij. Daarom moet de overheid verschillende expertises bij elkaar brengen. Dit vergt een verandering van een verzameling specialisten naar een meer generalistische blik op de organisatie en het stoppen met archiefjargon. Je hoeft geen archivaris te zijn om je bestanden goed op te slaan.

Ook aan de verhouding met inwoners moet de overheid nog sleutelen, willen we de burgerparticipatie bevorderen en inwoners goed kunnen betrekken bij de beleidsontwikkeling. Als overheid halen we nu wel veel informatie op, maar stoppen het vervolgens in onze eigen informatiesystemen waar de burgers weer niet bij kunnen. In beide gevallen van vernetwerking van de informatiesystemen is het van groot belang dat er vertrouwen is in elkaars expertise en goede wil. Door gebruik te maken van een gemeenschappelijke taal en uit te spreken waar het werkelijk over gaat, kunnen we de vertrouwensband aanhalen.

Een van de ideeën die is genoemd is het faciliteren van samenwerkingsverbanden en beleidsnetwerken. Door minder dezelfde dingen dubbel te doen kun je meer impact krijgen. Een goede samenwerkingsruimte en andere goed werkende digitale hulpmiddelen zijn hierbij van essentieel belang. Vanuit een dergelijke samenwerking kan beleidsuitwisseling ontstaan en resultaatgerichter gewerkt worden, bijvoorbeeld door gebruik te maken van een Scrum-methodiek. Je kunt ook een “vreemd beleid-app” gebruiken om af en toe met een rare gedachtecronkel

een nieuw idee te ontdekken en je gedachten te verrijken.

DEELSESSIE 2

Beleidsverfgoed – conceptueel terugkijken

Context van de ontwerpmissie

Aan het begin van de toenemende digitalisering is er te weinig aandacht geweest voor duurzame toegankelijkheid van informatie. Daardoor zijn er in de afgelopen 30 jaar puinhopen in de archieven ontstaan. Deze digitale achterstanden zijn nog steeds aan het groeien. Mede hierdoor staat de authenticiteit van overheidsinformatie onder druk. Om de digitale achterstanden te herstellen is het nodig dat we een digitale restaurator in het leven roepen die aan de slag gaat om de kwaliteit van informatie te verbeteren. Voor grote historische gebeurtenissen kan ook de hulp in worden geroepen van een digitaal archeoloog, die als taak heeft om de oude digitale wereld weer tot leven te wekken. Zij kunnen daarbij geholpen worden door een systeem als *reverse image searching*, dat Google gebruikt om vergelijkbare plaatjes te vinden op het internet. Ook kunnen automatische systemen voor waardenoekening en bronnencheck van

meerwaarde zijn voor dit traject. Om de authenticiteit van informatie te vergroten is het ook van belang om als beleidsbiograaf of *digital authenticator* te achterhalen welke veranderingen aan een document hebben plaatsgevonden. Hierbij moet niet alleen van de kennis van een expert gebruik worden gemaakt, maar dit door meerdere bronnen worden bekrachtigd. Dit kan worden bereikt met blockchain of andere vorm van digitale handtekening. De verschillende vormen van informatie (tekst, film, foto's of audio) kunnen met een digitale locatie worden weergegeven op een landkaart en gebruikt worden om tijdreizen te maken door je informatie.

Ten slotte is er nagedacht over manieren om de functionaliteit van het eDepot te koppelen aan werksystemen. Met behulp van automatisch gegenereerde sjablonen zou het mogelijk kunnen zijn om informatie vanaf de creatie al duurzaam toegankelijk te behouden. Met de druk op een rode knop op je toetsenbord kun je gelijk informatie duurzaam bewaren (met of zonder reminder) of we kunnen Artificial Intelligence (AI) laten bepalen of informatie bewaard moet worden voor de toekomst.

DEELSESSIE 3

Data-experiment – instrumenteel vooruitkijken

Context van de ontwerpmissie

Dit gebeurt in de omstandigheden dat er een overwaardering is op ict-geld, waardoor leveranciers de

macht hebben en er onvoldoende tijd en geld worden besteed om ict op een goede manier te implementeren.

In deze nieuwe basis moet er sectoroverstijgend gewerkt kunnen worden door het op een lijn krijgen van gescheiden werelden die nog niet elkaars taal spreken. Om dit te bereiken moet er binnen de overheid meer aandacht komen voor datakunstenaars en *data translators*.

Zij hebben als nobele taak om de informatie te transformeren naar concrete beelden, zodat het gesprek aangegaan kan worden met de burgers in de wijk, bibliotheek of supermarkt. Hiervoor moeten alle data en correspondentie op een handige manier worden verzameld in een "alles-dossier" voor de aanvrager van een informatieverzoek. Met behulp van een *blue button* kan de aanvrager bepalen met wie zijn informatie allemaal wordt gedeeld. Dit vergt van de overheid dat we beter worden in creatief nadenken en ons dienstbaar opstellen.

Om een data-experiment goed vorm te geven moeten we ook binnen de overheid de nodige veranderingen ondergaan. We moeten meer aandacht schenken aan de *data scientists* die bij ons werken en ook meer inzetten op datamanagement via een chief data officer. Zij kunnen ook samen met AI-ontwikkelaars in verschillende labs gaan werken aan overzichtelijke AI die de burger gaat helpen. Deze AI moet wel goed uitgelegd en getoetst kunnen worden zodat problemen worden voorkomen.

Lid worden?

Word lid van de KNVI

KNVI verbindt, verrijkt, versterkt

Het lidmaatschap van de KNVI is er voor iedereen, werkzaam in (of met belangstelling voor) het vakgebied informatiebeheer en/of archivering. Word lid en profiteer van:

- Het abonnement op het vakblad Od
- Gratis of tegen gereduceerd tarief deelnemen aan alle activiteiten van de KNVI
- Brede netwerk mogelijkheden met collega-informatieprofessionals

Binnen de KNVI is de interessegroep SOD actief voor informatiebeheerders bij de overheid.

Lidmaatschapsvormen

A Persoonlijk lidmaatschap
Contributie bedraagt € 176,49

B Organisatielidmaatschap;
contributie bedraagt:

- bij 1 – 6 fte: € 225,00 excl. btw
- bij 7 – 12 fte: € 500,00 excl. btw
- bij 13 – 24 fte: € 775,00 excl. btw
- bij 25 fte – >: € 1.380,00 excl. btw

Bij een organisatielidmaatschap ontvangt de organisatie een evenredig aantal abonnementen op Od.

Voor organisaties zijn er ook mogelijkheden om de SOD te sponsoren. Interesse? Neem contact op via info@knvi.nl



De SOD maakt sinds 1 januari 2017 deel uit van de verenigde beroepsverenigingen KNVI, Ngi-NGN en SOD

Postbus 1058
3860 BB NIJKERK
T: 033 247 34 27
E: info@knvi.nl
W: www.knvi.nl

OD KENNISSESSIE

12 APRIL 2022



THEMA

OFFICE 365 SHAREPOINT,
COMPLIANCE EN
RECORDSMANAGEMENT

- ✓ PLENAIRE SESSIES
- ✓ WORKSHOPS
- ✓ LEZINGEN
- ✓ VOLOP GELEGENHEID TOT NETWERKEN
- ✓ STANDS

Samen met 150 informatieprofessionals in de overheid kennis delen en verdieping zoeken. Een kans bij uitstek om ontwikkelingen in jouw vakgebied te bespreken en van elkaar te leren. Met keynotesprekers, ervaren praktijktrainers en docenten gaan we dieper op Office 365 SharePoint, compliance en recordsmanagement in.

Programma

09.45 – 10.45 uur	Plenaire opening door Eric Kokke met Eric Burger
10.45 – 12.00 uur	Workshopronde 1
12.00 – 13.00 uur	Lunch en netwerken
13.00 – 14.15 uur	Workshopronde 2
14.15 – 14.25 uur	Pauze en netwerken
14.25 – 15.40 uur	Workshopronde 3
15.40 – 16.15 uur	Plenaire lezing en afsluiting
16.15 – 17.00 uur	Netwerkborrel

Keynotespreker

Eric Burger, specialist in recordsmanagement en informatie governance in Office 365

Workshops

- **Joyce van Aalten**, specialist in taxonomieën en metadata, in het bijzonder in Office 365
- **Martijn Aslander**, technologie-filosoof en auteur van *Ons werk is stuk*
- **Eric Burger**, specialist in recordsmanagement en informatie governance in Office 365
- **Tom Haeck**, expert informatie- en archiefbeheer en lector aan de Arteveldehogeschool
- **Layla Hassan**, adviseur documentaire en digitale informatievoorziening bij het ministerie van Financiën
- **Eric Kokke**, GO Opleidingen/KNVI/RDDI
- **Rens Ouwerkerk**, adviseur Ontwikkeling Kennisproducten, Nationaal Archief

MELD JE AAN VIA

WWW.OD-ONLINE.NL/KENNISSESSIE

De Od Kennissessies zijn mogelijk gemaakt door

