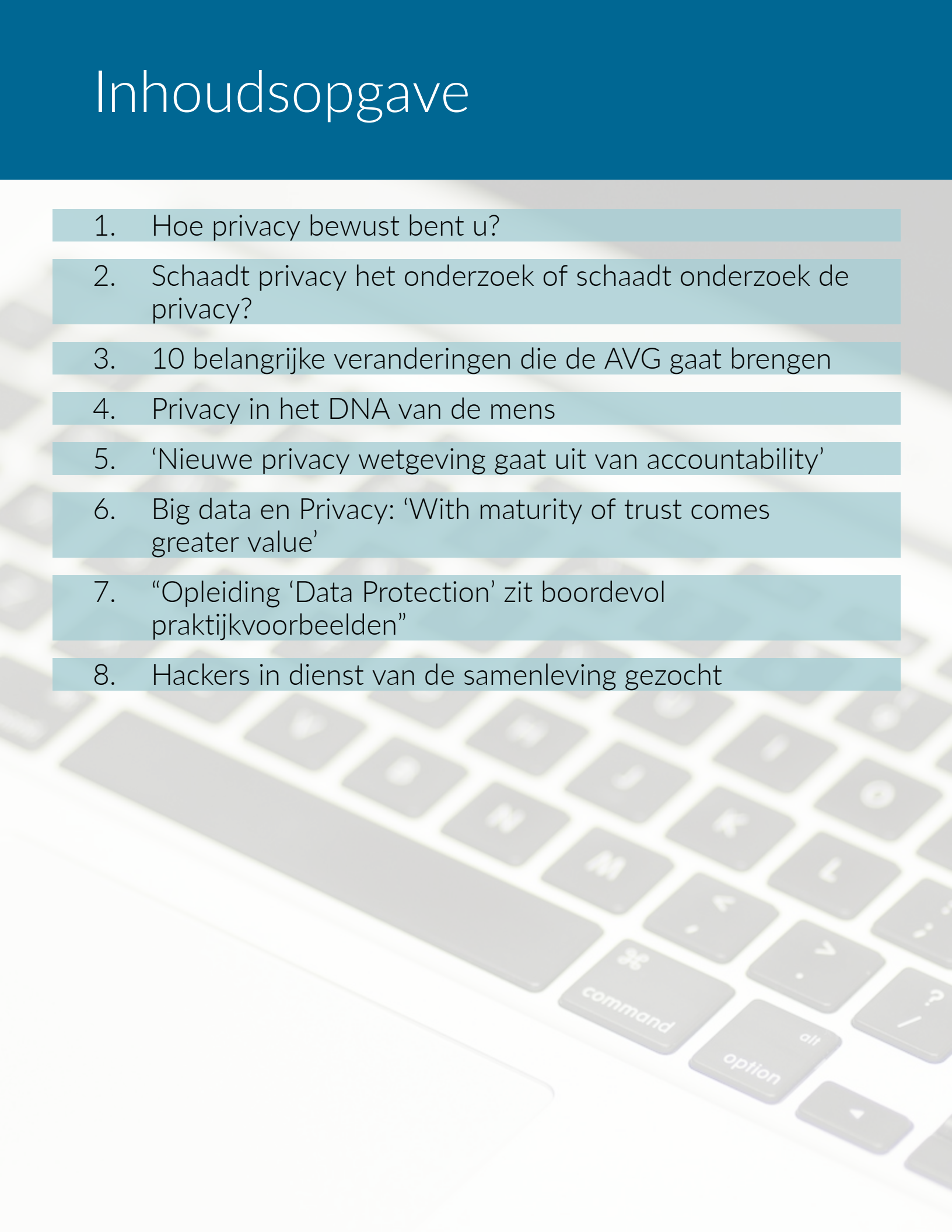
DATA UPDATE

eBook

Data & Privacy

Inhoudsopgave



Inleiding

Beste lezer,

Op 25 mei 2018 gaat met de invoering van de Algemene Verordening Gegevensbescherming (AVG) nieuwe wetgeving gelden in de gehele Europese Unie voor iedere organisatie, publiek of privaat voor het verwerken van persoonsgegevens. Dit heeft veel impact op de manier van gegevensverwerking binnen iedere organisatie.

Bedrijven en overheden moeten ervoor zorgen dat zij meer grip, controle krijgen en houden op wat er met persoonsgegevens gebeurt. Binnen hun eigen organisatie, maar ook als men data uitwisselt met andere organisaties.

In deze **Data Update** waarbij Data & Privacy centraal staat, vindt u een selectie artikelen die licht werpen op de impact van deze nieuwe wetgeving.

Wij wensen u veel leesplezier toe!

EUROFORUM

Hoe privacy bewust bent u?

Vorig jaar heeft NPO 3 veel aandacht besteedt aan het thema privacy in de privacyweken van 17 t/m 29 oktober 2016. Een thema dat zowel impact heeft op de bedrijfsvoering van organisaties, maar ook op de mens als individu. Wat vinden wij als burger van privacy? Hoe privacy bewust zijn we? Weten we welke informatie we allemaal vrijgeven? En belangrijker nog, wat doen de organisaties met onze gegevens?

In de privacyweken richt de NPO zich vooral op de mens als individu. Hoe gaan wij om met onze privacy? We roepen dat we niets te verbergen hebben. Maar is dat eigenlijk wel zo? Geven we tegelijkertijd niet veel van onze vrijheid op in ruil voor gemak en veiligheid? En zijn we ons eigenlijk wel bewust van alle informatie die wij prijsgeven?

Hoe privacy bewust bent u? Verschillende documentaires, films, series, maar ook presentaties van experts in het programma 'De Universiteit van Nederland' geven inzicht in het privacy bewustzijn.

Privacy bewustzijn in de organisatie

Ook in het bedrijfsleven is het thema privacy een hot item. Vanaf mei 2018 is een Data Protection Officer (DPO) / Functionaris Gegevensbescherming (FG) verplicht in de hele EU volgens de Algemene Verordening Gegevensbescherming (AVG). Deze verplichting geldt voor organisaties in de publieke sector en organisaties die zich toeleggen op extra privacygevoelige activiteiten. Voor overige organisaties is de aanstelling van een gekwalificeerde DPO een verstandige keuze.

Naast de aanstelling van een DPO of FG is kennis van privacywetgeving van belang. Op welke wijze voldoet uw organisatie aan de privacywetgeving? Hoe zorgt uw organisatie dat privacy ingebed wordt?

Om vanaf mei 2018 gereed te zijn voor de ingang van de AVG raden wij aan u tijdig voor te bereiden. Niet alleen omdat u zo hoge boetes en verscherpt toezicht door de landelijke Autoriteit Persoonsgegevens voorkomt. Maar vooral ook omdat een goede DPO/FG helpt om slimmer in te spelen op de uitdagingen van het digitale tijdperk.

Schaadt privacy het onderzoek of schaadt onderzoek de privacy?

In de aanloop naar 25 mei 2018, wanneer de Algemene Verordening Gegevensbescherming (AVG) van kracht gaat, worden we in media regelmatig herinnerd aan het feit dat 'bedrijven nog in onvoldoende mate compliant zijn met de AVG' en we zien aan de andere kant het aantal informatiebijeenkomsten en congressen gericht op verheldering van de verschillende aspecten in de AVG toenemen.

Het onderwerp 'privacy' is al lang niet meer alleen het onderwerp van de notoire voorvechters, maar wordt breed bediscussieerd. Het interessante boek: 'Je hebt wél iets te verbergen', van Maurits Martijn & Dimitri Tokmetzis, heeft hierbij een positief effect gehad, heb ik gemerkt.

Ook in Academia vraagt men zich af wat die AVG eigenlijk is, wat mag je wel en niet? Wie weet wat wel en niet mag? Ik hoor verschillende antwoorden op dezelfde vraag; wat moet ik nu? Kan ik eigenlijk nog wel onderzoek doen of wordt het nu praktisch onmogelijk?

De hamvraag beantwoord

Om de hamvraag maar gelijk te beantwoorden: onderzoek is nog steeds prima mogelijk. Eigenlijk is dat ook niet de juiste vraag. Omdat in de AVG de rechten van personen nu beter geborgd zijn en daarnaast rollen, verantwoordelijkheden en bevoegdheden in algemene zin beter zijn aangegeven in de AVG, geldt dat we onze verantwoordelijkheid moeten nemen als we met persoonsgegevens werken - ook in wetenschappelijk onderzoek. Zoals wij willen dat onze privacy beschermd wordt door bijvoorbeeld bedrijfsleven en overheid, mogen personen betrokken in ons onderzoek erop rekenen dat wij ook hun recht op privacy borgen, door het nemen van passende organisatorische en

technische maatregelen. Als onderzoeker, noch als instelling wil je de krant halen met datalekken vanwege je onderzoek. Omdat wetenschappelijk onderzoek in de regel een vorm is van internationale samenwerking, vaak ook publiek - privaat, met het oog op maatschappelijke relevantie en impact, is het borgen van privacy van burgers uit diezelfde maatschappij uiteraard niet ter discussie.

De vraag wordt daarmee: hoe kunnen we in ons wetenschappelijk onderzoek onze verantwoordelijkheid nemen en de privacy principes borgen?

De crux zit hem al in het ontwerp van het onderzoek

Door tijdig hulp in te schakelen van onderzoeksondersteuning binnen de instelling en een zogenaamde data protection impact assessment (DPIA) te doen, borg je dat je op een gestructureerde wijze de juiste methodologische, ethische en juridische afwegingen maakt.

Je bepaalt enerzijds de impact van de rechten van de betrokkenen (de personen betrokken in je onderzoek) en je neemt passende maatregelen - en documenteert dit in je data management plan.

Tenslotte gelden er specifiek voor wetenschappelijk onderzoek, en voor statistische bewerkingen en archivering, bepaalde uitzonderingen, die recht doen aan de praktijk van het bedrijven van wetenschap.

Instrumenten en technische maatregelen

Naast de DPIA, geeft de AVG instrumenten en technische maatregelen aan die recht doen aan het borgen van privacy in de verwerking van persoonsgegevens. Hierbij speelt de functionaris gegevensbescherming (FG), ook beschreven in de AVG, een belangrijke rol binnen je instelling. Er ontstaan steeds meer rollen in de ondersteuning van onderzoek, zoals juridisch adviseurs met kennis van zowel onderzoek als gegevensbescherming en bijvoorbeeld ook intellectueel eigendom en auteursrecht, waardoor de onderzoeker door de instelling in de gelegenheid wordt gesteld om in zijn of haar onderzoek recht te doen aan verantwoorde omgang met persoonsgegevens, in de zin van de AVG. Met adviezen, met contracten en overeenkomsten en met goede risico-inschattingen en passende tegenmaatregelen bijvoorbeeld.

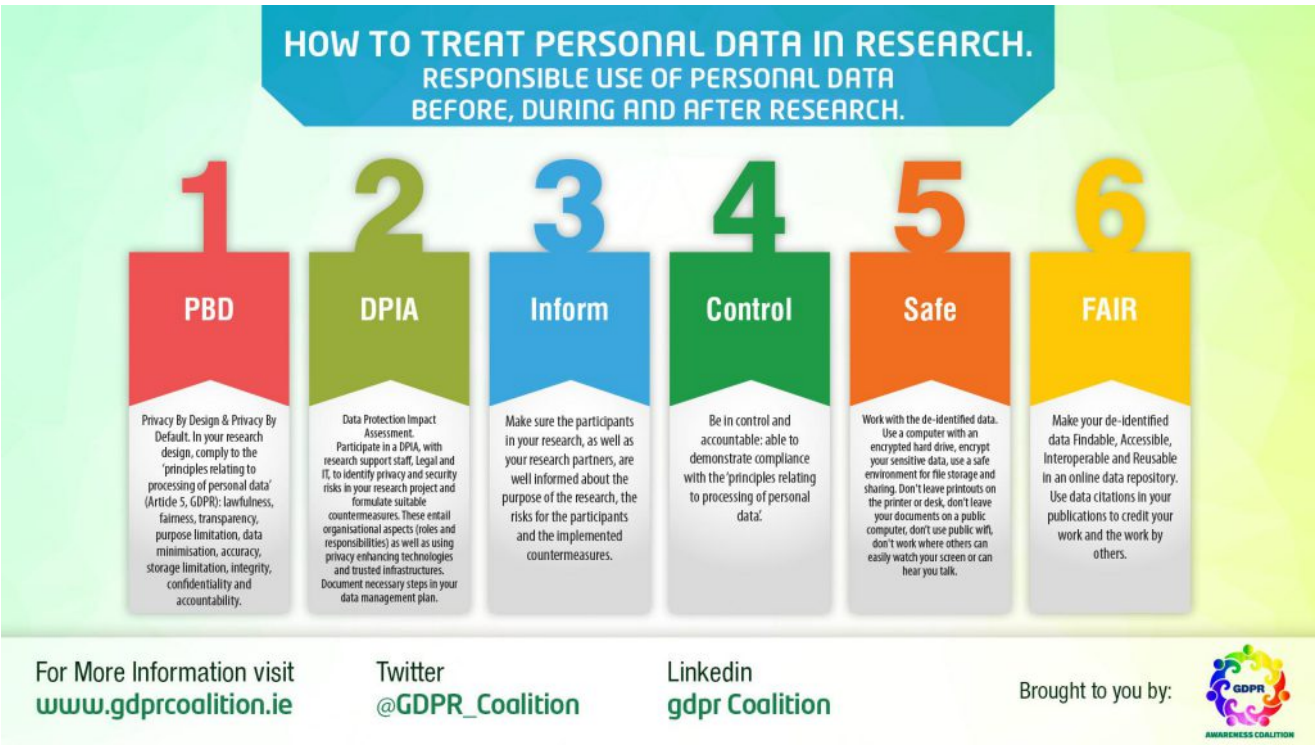
Hierbij speelt de beschikbaarheid van technische voorzieningen een niet onbelangrijke rol. Kun je ook daadwerkelijk data veilig opslaan, encrypten en beveiligd gegevens uitwisselen? Weet je hoe je moet anonimiseren of pseudonimiseren en wanneer? Hoe werkt je software met dergelijke data en waar staan die data?

Herziening VSNU gedragscode

Momenteel wordt de VSNU gedragscode omgang persoonsgegevens in wetenschappelijk onderzoek herzien. Deze code zal praktische handvatten geven aan onderzoekers, hoe in deze te onderscheiden onderzoekscenario's verantwoord om te gaan met persoonsgegevens?

Dus bijvoorbeeld voor survey onderzoek, voor onderzoek op basis van CBS data, voor big data onderzoek op basis van data van social media en onderzoek op basis van observaties van minderjarigen. Deze komt in oktober 2017 beschikbaar voor publieksconsultatie.

Neem hier bijvoorbeeld goed kennis van en gebruik een dergelijk document om binnen je onderzoeksgroep, vakgroep, faculteit, instelling te bepalen hoe je als professional accountability kunt demonstreren en transparant kunt zijn over de wijze waarop je je onderzoek inricht en uitvoert.



***Geschreven door: Marlon Domingus**, project manager research data management (RDM) bij de Erasmus Universiteit Rotterdam en leider van de RDM community.*

10 belangrijke veranderingen die de AVG gaat brengen

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Als het gaat om de verwerking van persoonsgegevens hebben we vanaf dat moment niet meer te maken met de Wet bescherming persoonsgegevens, maar met nieuwe regels die in de hele Europese Unie gelijk zijn. Wat betekent dat?

1. Een verordening in plaats van een richtlijn

In Europa vinden we op dit moment de regels voor de verwerking van persoonsgegevens in de nationale privacywetten waarmee lidstaten de Privacyrichtlijn 95/46/EG van 24 oktober 1995 hebben omgezet. Deze Privacyrichtlijn verlangt van lidstaten dat zij ervoor zorgen dat hun wetgeving waarborgen bevat 'in verband met de verwerking van persoonsgegevens' en dat dit gebeurt 'overeenkomstig de bepalingen van de richtlijn'.

In Nederland is dat gebeurd in de Wet bescherming persoonsgegevens (Wbp) en ook wel in andere wetten, zoals de Wet basisregistratie personen. In België is dat gedaan in de Wet verwerking persoonsgegevens, in Frankrijk in de *Loi informatique et libertés*, in het Verenigd Koninkrijk in de *UK Data Protection Act 1998* en in Zweden in de *Personuppgiftslagen*. Enzovoorts. En al deze wetten wijken op onderdelen van elkaar af. Er is daardoor sprake van fragmentatie en dat is om allerlei redenen onwenselijk. De verordening wil daaraan wat doen door alle nationale privacywetten te vervangen door een verordening, die rechtstreeks verplichtingen oplegt aan degenen die persoonsgegevens verwerken.

Wat betekent dat? **Een set van regels betekent veel meer consistentie in Europa, en daarmee meer rechtszekerheid. Toch moet ermee rekening worden rekening gehouden dat de toepassing van de regels in verschillende lidstaten uiteen kan lopen.** Dit enerzijds doordat de verordening lidstaten bij sociale zekerheid, arbeid en zorg toch nog veel ruimte geeft om eigen regels vast te stellen. En anderzijds doordat de verordening, zoals alle privacywetgeving, zich kenmerkt door veel open begrippen en vage normen, die op nationaal niveau worden ingevuld.

2. Enkele nieuwe begrippen

De verordening introduceert enkele nieuwe begrippen. Soms gaat het om nieuwe aanduidingen voor inhoudelijk ongewijzigde begrippen. Enkele andere begrippen waren nog niet in de richtlijn opgenomen, maar werden al wel gebruikt. En weer enkele andere begrippen zijn helemaal nieuw, in zoverre dat daarvoor in de verordening een nieuwe begripsomschrijving wordt gegeven.

Zo gaan de 'verantwoordelijke' voortaan aanduiden als 'verwerkingsverantwoordelijke' en de bewerker als 'verwerker'. We zullen er wel aan wennen, zoals we ook wel gewoon zullen worden met 'bindende bedrijfsvoorschriften' en de gegevensbeschermingseffect-beoordeling'. Verder is betrekkelijk nieuw begrippen als 'profilering' (art. 4(4) AVG), 'pseudonimisering', alsmede 'genetische gegevens' en 'biometrische gegevens' Allemaal begrippen die in de verordening eigen specifieke regelingen hebben gekregen.

3. Vergrote materiële werkingssfeer (?)

De materiële werkingssfeer van de nieuwe regels komt overeen met die van de huidige regels. De verordening is, evenals de richtlijn, van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand ('een gestructureerd geheel van persoonsgegevens') zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Evenals in de richtlijn voorziet de verordening in een handvol uitzonderingen. Zo zijn de regels niet van toepassing op de gegevensverwerkingen op activiteiten betreffende de openbare veiligheid, defensie, de staatsveiligheid en dergelijke. En evenmin op verwerkingen door politie en justitie met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. En ten slotte ook niet op verwerkingen door natuurlijke personen bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.

In zoverre niets nieuws dus. Echter, in het wetgevingsproces zijn wel voorstellen gedaan die beoogden de werkingssfeer van de regels op te rekken door de definitie van wat persoonsgegevens zijn uit te breiden tot de gegevens betreffende natuurlijke personen die kunnen worden onderscheiden van anderen (in het Engels: *singled-out*). Uiteindelijk is het niet zo ver gekomen. Uit de preambule van de verordening kan worden opgemaakt dat er géén sprake van persoonsgegevens als het gaat om gegevens die betrekking hebben op iemand waarvan de identiteit niet zonder onevenredige inspanning kan worden achterhaald.

Ook niet als die persoon bijvoorbeeld met behulp van een IP-adres of andere apparaat-identifier kan worden onderscheiden van anderen. Van belang is wel dat toezichthouders er moeite mee hebben dit te accepteren en nog steeds al heel snel geneigd zijn om gegevens al snel op te vatten als persoonsgegevens, al was het maar omdat zij alleen dan bevoegd kunnen zijn om op te treden...

4. Uitbreiding territoriale werkingssfeer

Wanneer zijn de nieuwe regels van toepassing als persoonsgegevens niet in Europa worden verwerkt? Onder de huidige regels geldt daarvoor een betrekkelijk ingewikkelde regeling, waarbij wordt gekeken naar de activiteiten van de vestiging van de verwerkingsverantwoordelijke. Deze regeling blijft, zij het in iets gewijzigde vorm, en in zoverre verandert er dus niet heel veel.

Er wordt wel een gemakkelijk te begrijpen regeling aan toegevoegd, op grond waarvan de nieuwe regels ook van toepassing gaan zijn als een verantwoordelijke van buiten Europa zich richt op individuen in de Europa. Het is daarmee zonder meer duidelijk dat onze privacyregels van toepassing zijn op Google, Facebook of Whatsapp -- iets wat onder de huidige regels vaak nog tot discussie kon leiden.

5. Meer verplichtingen voor verwerkers

Een typisch voorbeeld van een bewerker of verwerker is Workday of Salesforce. **Een verwerker verwerkt persoonsgegevens ten behoeve van een verantwoordelijke, die de zeggenschap heeft over de gegevens. Onder de nieuwe regels krijgen verwerkers te maken met veel meer verplichtingen.** Het onder meer om verplichtingen

- met betrekking tot het gebruik van sub-verwerkers;
- het informeren van de verantwoordelijke over datalekken;
- documentatie van gegevensverwerkingen (data-mapping);
- om een functionaris voor de gegevensverwerking aan te stellen;
- met betrekking tot gegevensdoorgiften naar landen buiten de unie.

Deze nieuwe verplichtingen maken het mogelijk dat toezichthouders en betrokkenen zo nodig ook een verwerker kunnen aanspreken als er iets mis is gegaan met de door hen verrichte gegevensverwerkingen. Onder de huidige regels konden ze vaak alleen de verantwoordelijke aanspreken.

6. Meer (en meer gedetailleerde) rechten voor betrokkenen

Op dit moment hebben betrokkenen allerlei rechten die zij tegenover de verantwoordelijke kunnen inroepen. Het gaat dan om inzage en verbeterings- of verwijderingsrechten, en het daaruit afgeleide vergeetrecht, alsmede verzetsrechten met betrekking tot geautomatiseerde besluitvorming of direct marketing.

In de verordening zien we al deze rechten in meer uitgewerkte en gedetailleerde vorm terug. Onder de nieuwe regels moet er veel meer informatie aan betrokkenen worden verstrekt, onder andere over bewaartermijnen, klachtrechten en -procedures, gegevensdoorgiften naar landen buiten de unie en de in dat verband getroffen waarborgen, en het bestaan van de mogelijkheid dat er geautomatiseerde besluitvorming en profilering plaatsvindt.

Verder voorziet de verordening in een aantal heel nieuwe rechten voor betrokkenen. Wat daarvan vooral opvalt zijn het gegevenswissingsrecht ('recht op vergetelheid') en het recht op gegevensoverdraagbaarheid, dat de betrokkene het recht geeft om in bepaalde gevallen de gegevens die hij heeft verstrekt aan de éne verwerkingsverantwoordelijke te doen overdragen naar de andere.

7. En nogal wat formaliteiten

De verordening voorziet in nogal wat verplichtingen die ik gemakshalve maar samenvat onder de noemer 'formaliteiten', zonder dat ik daarmee de suggestie willen wekken dat deze geen of weinig waarde hebben. **Het zijn de verplichtingen die verband houden *accountability*, het kunnen aantonen dat er is voldaan aan de wettelijke vereisten.** Er kan worden gedacht aan de verplichtingen om een register van verwerkingsactiviteiten bij te houdenof om een gegevensbeschermingseffectbeoordeling te doen. Ook de verplichting om een functionaris voor de gegevensbescherming aan te stellen, kent nogal wat formele vereisten, bijvoorbeeld met betrekking tot zijn of haar rechtspositie, takenpakket en verantwoording.

Een risico van dit soort formaliteiten is dat deze bijdragen aan een bedrijfscultuur waarin erop wordt vertrouwd dat het met de gegevensbescherming wel goed zit als in de privacyverklaring alle verplichte onderwerpen zijn benoemd, zolang de vragenlijsten van de gegevensbeschermingseffectbeoordelingen netjes zijn ingevuld, zolang er iemand

is met op haar visitekaartje de titel DPO. Enzovoorts

8. Ook meer instrumenten voor internationale doorgifte

De verordening bevat, evenals de richtlijn, een verbod op de doorgifte van persoonsgegevens naar landen buiten de Europese Unie, of eigenlijk de Europese Economische Ruimte (EER), die geen passend beschermingsniveau bieden. Wat dat betreft verandert de verordening niet veel aan de situatie onder de richtlijn. Wel voorziet de verordening in meer instrumenten die het mogelijk maken om persoonsgegevens door te geven naar landen die geen passend beschermingsniveau bieden. In aanvulling op de al bekende modelcontracten en binding corporate rules ('bindende bedrijfsvoorschriften') kan onder de nieuwe regels ook gebruik worden gemaakt van gedragscodes en certificeringsmechanismes.

In de verordening wordt vervolgens nog wel een nieuwe uitzondering op het doorgifteverbod geïntroduceerd. In uitzonderlijke gevallen kan een doorgifte ook zijn toegestaan zijn als is voldaan aan de volgende, tamelijk strenge voorwaarden: (i) de doorgifte mag niet repetitief zijn en (ii) het aantal betrokkenen moet beperkt zijn; (iii) de doorgifte moet nodig zijn voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene; (iv) en de verwerkingsverantwoordelijke moet alle omstandigheden in verband met de gegevensdoorgifte hebben beoordeeld en op basis daarvan passende waarborgen voor de bescherming van persoonsgegevens hebben geboden. Als gebruik wordt gemaakt van deze uitzondering moet de verwerkingsverantwoordelijke ten slotte ook de nationale toezichthouder en de betrokkenen daarover informeren.

9. Het Europees Comité voor Gegevensbescherming

De Art. 29 Werkgroep bestaat uit vertegenwoordigers van de nationale toezichthouders in de verschillende lidstaten en van de Commissie en andere EU-instellingen. De werkgroep wordt geacht onafhankelijk te zijn en raadgevend van aard, en is vooral bekend van de adviezen of opinies die het publiceert over de uitleg van begrippen uit de richtlijn.

In de verordening wordt de werkgroep het Europees Comité voor Gegevensbescherming en krijgt het meer taken en bevoegdheden. Zo kan het Comité richtsnoeren vaststellen en aanbevelingen doen, beste praktijken (bedoeld zijn *best practices*) opstellen, en dat allemaal gevraagd en ongevraagd. Wat nieuw is, althans onder de richtlijn niet uit de verf is gekomen, is dat het Comité gaat bevorderen dat er

gedragscodes tot stand komen. Ook is nieuw dat het zich gaat bezighouden met accreditatie van certificeringsorganen en van de periodieke evaluatie ervan.

10. En ten slotte substantiële boetes

Er is betrekkelijk veel aandacht voor de boetes die nationale toezichthouder onder de verordening kunnen gaan opleggen aan verwerkingsverantwoordelijken en verwerkers voor overtredingen van de bepalingen uit de verordening. Dat is wellicht terecht. Als sluitstuk op de handhaving zijn deze boetes waarschijnlijk bepalend voor de naleving van de verordening. Er zijn twee boetecategorieën:

- Er zijn boetes van ten hoogste €10 miljoen of 2 procent van de wereldwijde omzet van de verwerkingsverantwoordelijke of verwerker.
- En er zijn boetes van ten hoogste €20 miljoen of 4 procent van de wereldwijde omzet.

***Geschreven door**: **Gerrit-Jan Zwenne,** hoogleraar Recht en de informatiemaatschappij aan de Universiteit Leiden en advocaat bij Brinkhof in Amsterdam.*


EUROFORUM
Volledig op de hoogte van Data & Privacy
Euroforum organiseert diverse opleidingen en congressen met betrekking tot Data & Privacy.
Bekijk het complete aanbod

Privacy in het DNA van de mens

In een wereld waarin we dankzij de modernste communicatietechnologieën gegevens razendsnel met elkaar kunnen delen, wordt het risico ook steeds groter dat gegevens in handen van de verkeerde komen te vallen. Natuurlijk is er veel technisch te regelen wat betreft beveiliging van gegevens, maar vaak blijft het toch mensenwerk. **Hoe zorg je er nou voor dat mensen de sterkste schakel binnen een bedrijf worden? Het begint allemaal met awareness.**

Oeps…dat was een beetje dom

***Voorbeeld I**: Een inbreker breekt in, in de auto van een medewerker. De buit: een werklaptop en een mobiele werktelefoon. Erg vervelend voor de medewerker in kwestie, maar ook voor het bedrijf waar deze persoon werkt. Het kan namelijk zo zijn dat er op de laptop en op de telefoon allerlei gegevens, waaronder persoonsgegevens en gevoelige bedrijfsinformatie staan.*

***Voorbeeld II**: Een medewerker krijgt een mailtje van een onbekende afzender met daarin een link, waar hij onnadenkend op klikt. Gevolg: hackers dringen op afstand de computer binnen en "gijzelen" bestanden op zijn computer, het zogenaamde ransomware. De hackers sturen een bericht waarin ze geld eisen voordat ze de bestanden weer toegankelijk maken.*

Het zijn niet alleen dit soort incidenten waardoor het steeds belangrijker wordt om informatie en persoonsgegevens goed te beveiligen. Zo is het al lang niet meer gebruikelijk om alleen achter jouw bureau op kantoor te werken, maar ook elders in het pand, of zelfs op plekken buiten kantoor. Het is natuurlijk erg fijn dat je bijvoorbeeld vanuit huis kunt werken, maar die bewegingsvrijheid brengt ook extra risico's met zich mee voor de informatie waarmee mensen werken. **Niet alleen via technische communicatiemiddelen kunnen gegevens in ongewenste handen vallen.**

Ook via persoonlijke gesprekken kan informatie naar buiten lekken en mogelijk schade veroorzaken. Stel dat een iemand in de trein aan de telefoon over bijvoorbeeld een andere college praat of over een op handen zijnde reorganisatie.

Als bedrijf kun je dit soort communicatie natuurlijk niet beveiligen, maar je kan wel proberen iedereen bewust te maken van de impact die het kan hebben als je niet voorzichtig met gegevens omgaat. Maar hoe doe je dat?

Awareness

Belangrijk is om eerst vast te stellen wat de mate van "maturity" is van jouw bedrijf als het om omgang met gegevens gaat. Daartoe kun je bijvoorbeeld een nulmeting uitvoeren met een door iedere medewerker in te vullen vragenlijst. Denk aan vragen als "Ben je je er van bewust dat je met persoonsgegevens werkt? en "Weet je wat het beleid van het bedrijf is ten aanzien van het werken met (persoons) gegevens?". De resultaten van de vragenlijst geven een beeld van de kennis en kunde die er bij de medewerkers is. Met dat beeld kan je weer vaststellen aan wat voor informatie er behoefte is binnen jouw bedrijf. Zo kan je je awareness-programma daar weer op aanpassen. **Want het begint allemaal met het "aware" maken van mensen.**

Neem ze in presentaties mee in de wondere wereld van privacy. En houd de "awareness"op peil. Maak er een jaarlijks iets van, bijvoorbeeld met een e-learning module. Naast het trainen van mensen, kan je ook een privacy-dag organiseren of grappige gadgets uitdelen. Privacy moet gaan leven bij mensen. Het moet echt in hun DNA gaan zitten. Even weg van mijn bureau? Dan ook mijn computer locken! In de trein werken? Geen gevoelige zaken bespreken! Natuurlijk is dit niet iets wat overnacht gebeurt, maar kost het tijd, veel tijd. De tijd en moeite is het echter meer dan waard, het gaat namelijk om jouw bedrijf.

***Geschreven door: Aleksandra N. Hornstra**, Legal Counsel en Privacy Officer, Sanquin*

‘Nieuwe privacy wetgeving gaat uit van accountability’

De huidige privacywetgeving is veranderd, maar wat is nou eigenlijk de impact van de nieuwe privacywet? Deze vraag stelde wij aan Gerrit-Jan Zwenne, hoogleraar recht en de informatiemaatschappij, Universiteit Leiden en advocaat te Amsterdam.

De belangrijkste veranderingen

De nieuwe privacywet is een aanmerkelijke uitbreiding en verfijning van de huidige wetgeving. De wetgeving is veel gedetailleerder en verlangt dat er meer wordt gedocumenteerd. En daarbij kunnen er onder de nieuwe wetgeving heel substantiële boetes worden opgelegd voor overtredingen. Organisaties die persoonsgegevens verwerken -- en welke organisatie doet dat nou niet? --- moeten dus precies gaan vastleggen welke gegevens ze verwerken, voor welke doeleinden, aan wie die worden verstrekt en van welke anderen organisaties daarbij gebruik wordt gemaakt. Er worden veel nieuwe eisen gesteld aan de inhoud van het privacy statement. Daarin moeten bijvoorbeeld straks ook de verschillende bewaartermijnen worden opgenomen.

Tot slot moeten heel veel organisaties bij zowel de overheid als het bedrijfsleven een functionaris voor gegevensbescherming (FG) benoemen. En die persoon (m/v) gaat zich ook bemoeien met allerlei zaken met betrekking tot de wijze waarop wordt omgegaan met persoonsgegevens. Dat is haar of zijn taak. Op allerlei niveaus moet worden voorzien in procedures om de wetgeving na te leven. We spreken dan van accountability.

Impact voor de financiële sector

De financiële sector is al zwaar gereguleerd, met krachtige toezichthouders als AFM en DNB. Financiële instellingen zijn bijna per definitie gegevensintensieve organisaties, die de beschikken over veel vaak betrekkelijk gevoelige gegevens die al snel kwalificeren als persoonsgegevens. Het gaat bij banken om transactie- en betaalgegevens en bij verzekeraars om gegevens over de woonsituatie of de wijze waarop gebruik wordt gemaakt van motorvoertuigen. Of gegevens over de gezondheid als het gaat om zorgverzekeraars. **De komst van PSD2 gaat weer nieuwe extra dimensies brengen.**

In dezelfde periode waarin de nieuwe privacywetgeving gaat gelden krijgt PSD2 betekenis. Nieuwe aanbieders, met nieuwe diensten en producten, gaan met toestemming van de rekeninghouder gebruik maken van betaalgegevens. Uiteraard moeten ook deze aanbieders voldoen aan de privacywet. Ook kunnen we verwachten dat de banken die de betaalgegevens verstrekken ervoor zorgdragen dat dit op een goede en zorgvuldige wijze gebeurt.

Advies aan organisaties:

Alles begint met bewustwording of 'awareness'. Er moet het besef zijn dat deze wetgeving er is en betekenis heeft. En dan volgt, als het goed is, de rest. Dat zal niet vanzelf gaan. **Waar ik veel van verwacht is de benoeming van een FG. Dat is bij uitstek de persoon die eraan kan bijdragen dat op een behoorlijke en zorgvuldige wijze wordt omgegaan met persoonsgegevens.**

***Geschreven door: Gerrit-Jan Zwenne**, hoogleraar Recht en de informatiemaatschappij aan de Universiteit Leiden en advocaat bij Brinkhof in Amsterdam.*

Big data en Privacy: 'With maturity of trust comes greater value'

Big data en data analytics *are here and here to stay.* **Alleen wanneer er vertrouwen is in de maatschappij in de wijze waarop data worden gebruikt doorondernemingen, in wat zij 'beloven' ten aanzien van privacy, is het mogelijk om de potentie van big data en de ontsluiting daarvan door data analytics volledig uit te nutten en waarde te creëren; om '*shared value*' te creëren**. De publiciteit naar aanleiding van uitingen van het Verbond van Verzekeraars, laat dat ook weer duidelijk zien. Batig aan het (bouwen aan) vertrouwen zijn *Privacy Impact Assessments*, toepassing van *Privacy by Design* en het acteren op de verwachtingen van de stakeholders van de onderneming. Transparantie en de overtuiging dat de onderneming '*keeps to its promisses*' is daarbij essentieel. *'With maturity of trust comes greater value'*.

Echter nog niet alle vraagstukken met betrekking tot privacy en big data en data analytics zijn beantwoord, zeker niet op de scheidslijn van de wettelijke kaders en de mogelijkheden van de techniek. Dit klemt nu sanctionering middels bijzonder hoge boetes (tot wel 5% van de wereldwijde omzet van een onderneming wordt) van niet naleving van deze wettelijke kaders mogelijk wordt, alsook gegeven het feit dat andere jurisdicties veelal een ander zogenaamd *dicovery and litigation* regime kennen.

Big Data en Vertrouwen

"*Do you do what you have promised to your stakeholders?"* Het is deze uitspraak die de essentie weergeeft van waardecreatie, het moderne winstbegrip. Waardecreatie staat voor de waarde die wordt gegenereerd voor alle stakeholders. Waardecreatie veronderstelt een direct verband tussen de (executie van de) strategie van de onderneming en (het voldoen aan) de verwachtingen van de stakeholders. **Dus waar privacy en het tegelijkertijd volledig uitnutten van de potentie van big data en data analytics innerlijk tegenstrijdig lijken dan wel zo worden gepercipieerd, namelijk het economisch belang vis-a-vis het belang van de bescherming van de persoonlijke levenssfeer, creëren beiden waarde voor de onderneming, voor haar respectievelijke stakeholders, maar alleen dan wanneer het vertrouwen wordt gehonoreerd: *'Building trust is creating shared value'*.**

Voor de ontwikkeling van big data en data analytics-toepassingen wordt het belang van vertrouwen alleen maar groter. In de Europese Data Protectie Verordening wordt getracht invulling aan dit vertrouwen te geven.

Big Data en Privacy

Een belangrijke vraag die rijst bij big data en data analytics is of de huidige juridische kaders en de Verordening (nog) aansluiten op de huidige stand en snelheid van ontwikkelingen van de techniek en vervolgens of de risico's verbonden aan big data en data analytics kunnen worden gemitigeerd om een optimale waardecreatie voor alle stakeholders door ondernemingen vanuit big data en data analytics te realiseren. **Wanneer we spreken over privacy in het kader van big data en data analytics, is het van belang om een onderscheid te maken tussen enerzijds de *bescherming van de persoonlijke levenssfeer* van individuen en anderzijds de *bescherming van persoonsgegevens* van individuen**.

Beiden raken aan de privacy van ons allen als individu, maar daar waar de bescherming van persoonsgegevens en het daarbij horende wettelijke kader vooral een issue is in de fase van verzamelen en analyseren van big data, raakt juist het toepassen van de analyses van big data aan de persoonlijke levenssfeer van individuen. Voor beiden geldt een *'ander'* juridisch kader.

In de vele bespiegelingen die er in verband met big data reeds zijn gemaakt, wordt vooral ingezoomd op de bescherming van persoonsgegevens en het feit dat ontwikkelingen in big data ertoe kunnen leiden dat steeds meer gegevens verworden tot persoonsgegevens. Dit omdat door het combineren van grote datasets waarin geanonimiseerde gegevens zitten, herleidbaarheid van de gegevens tot een individu toch ontstaat en op dat moment de gegevens zouden gaan kwalificeren als persoonsgegevens. Minder wordt stilgestaan bij het wettelijk kader ten aanzien van de bescherming van de persoonlijke levenssfeer van individuen. Dit kader kan, althans in mijn visie, mede een contra-balans vormen voor het ongebreidelde gebruik van big data, en kan juist gewetensvol en voorzichtig gebruik van big data en data analytics triggeren.

Establishing and safeguarding the *required trust*; amending the risks

Welke waarborgen maken c.q. kunnen maken dat er door het gebruik van big data en data analytics *shared value* wordt gecreëerd. Dit vermits de onderneming *keeps to its promisses?* **De (toepassing van de) huidige wettelijke kaders sluiten, in mijn visie als gezegd, onvoldoende aan bij het fenomeen big data; de ontsluiting daarvan door gebruikmaking van data analytics en de toepassing van de uiteindelijke analyses**. Niet alleen non-compliance met het wettelijk kader, en *subsequent loss* van reputatie of assets, is een risico bij het gebruik van van big data en data analytics. Immers tegelijkertijd bestaan de risico's, de

down sides, ook in het niet (kunnen) benutten van big data en data analytics, in de *loss of competitiveness*: "*The use of big data will become a key basis of competition and growth for individual firms. (…) From the standpoint of competitiveness and the potential capture of value, all companies need to take big data seriously,*

In dit verband en om daadwerkelijk *shared value* te bewerkstelligen, is het dan ook interessant om te bezien welke maatregelen zouden kunnen leiden tot waarborgen om alsnog de persoonlijke levenssfeer en persoonsgegevens van individuen te beschermen en tegelijkertijd voormelde risico's te mitigeren en de kansen die big data en data analytics bieden niet (volledig) teniet te doen.

In mijn visie liggen die maatregelen vooral op het gebied van accountability omdat transparantie, controle en (het nemen van) verantwoordelijkheid hierin samenkomen. *Privacy Impact Assessments* alsmede het vereiste van *Privacy by Design* zijn hier een mooi voorbeeld van. Het gaat daarbij in essentie om het door onderneming in de ontwikkelingsfase, in het ontwerp van big data en data analytics-toepassingen, meenemen van de privacyvereisten en bovenal in mijn visie ook van de verwachtingen van de stakeholders van de onderneming.

Deze zien niet alleen op de bescherming van hun gegevens, maar bovenal op de bescherming van hun persoonlijke levenssfeer en de zeggenschap die zij daarover hebben. Transparantie over wat, waarvoor er door wie met hun gegevens gebeurt en de overtuiging dat de onderneming *'keeps to its promisses'* is daarbij essentieel... *With maturity of trust comes greater value.*

Geschreven door: Monique G.M. van Dijken Eeuwijk, *Advocaat bij NautaDutilh; Voorzitter van het Benelux Sector Team Professional Services Firms en lid van het Privacy en E-commerce team*

“Opleiding ‘Data Protection’ zit boordevol praktijkvoorbeelden”

Theorie is pas werkelijk nuttig als je weet hoe je deze moet toepassen. Daarom zijn de docenten van de verkorte opleiding Data Protection voor Financials als geen ander thuis in de praktijk. Neem advocaat Cathérine Jakimowicz. Ze is gespecialiseerd in privacy en alles wat met de wet bescherming persoonsgegevens te maken heeft. “We gaan veel praktijkvoorbeelden geven, zodat cursisten weten waar de risico’s zitten en hoe je daarmee omgaat.”

Veel financiële instellingen willen als zij nieuwe producten en diensten ontwikkelen advies over hoe ze moeten omgaan met persoonsgegevens. Ook hebben ze vragen over de rechten van klanten, zoals het inzagerecht en het correctierecht. Vaak komen ze dan uit bij een expert, bijvoorbeeld Cathérine Jakimowicz. “Financiële instellingen willen weten hoe ze op de juiste manier opvolging moeten geven aan de regels. Verder hebben veel instellingen vragen over veranderende wet- en regelgeving. Die veranderingen raken de manier waarop financiële instellingen gegevens verwerken.”

Gevolgen privacyregels

Uit de nieuwe regelgeving die op 25 mei 2018 van kracht wordt, vloeien tal van verplichtingen voort. Jakimowicz: “Twee zaken zijn hierbij belangrijk. Allereerst: dat je als financiële instelling je risicoprocessen op orde hebt en dat kunt laten zien. Daarnaast is het belangrijk dat medewerkers van financiële instellingen weten dat er privacyregels zijn, wat deze regels inhouden en wat het gevolg van die regels is voor hun eigen werk. Daar staan we in deze cursus uitgebreid bij stil.”

Vragen uit de praktijk

De cursus, die eind november start, is doorspekt met praktijkvoorbeelden. “Mijn collega-docent Marta Borrat i Frigola werkt als jurist bij ABN AMRO Bank. Zelf werk ik veel voor financiële instellingen, ook in huis. We geven veel praktijkvoorbeelden, zodat de theorie gaat leven en cursisten begrijpen hoe je de theorie toepast. Hoe informeer je de klant afdoende over wat er met zijn persoonsgegevens wordt gedaan?

Waarvoor mag je gegevens gebruiken binnen een financiële instelling? Wat moet je inregelen bij nieuwe diensten die raadpleegbaar zijn via een app? Hoe moet je omgaan met inzageverzoeken of verzoeken om een BKR-registratie of EVR-registratie te verwijderen? Ook staan we stil bij nieuwe regelgeving zoals PSD2 en de privacy-uitdagingen die daar bij horen. ”

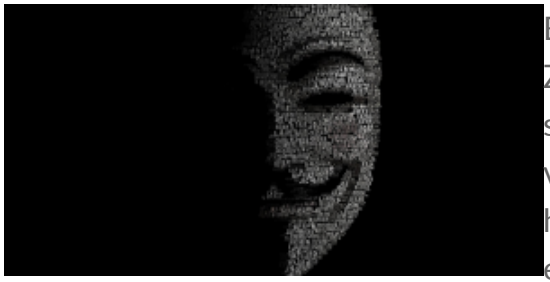
Praktische toepassing

Wat hebben cursisten na afloop geleerd? Jakimowicz: “Deelnemers begrijpen de privacyregels niet alleen, maar zijn na de opleiding ook in staat deze regels praktisch toe te passen. Ze kennen de risico’s , weten hoe je deze moet mitigeren en hoe je bepaalde vraagstukken oplost.

***Met dank aan: Cathérine Jakimowicz**, Advocaat partner bij SteensmaEven*

Hackers in dienst van de samenleving gezocht

Nu het digitale landschap steeds complexer wordt, zijn bedrijven en publieke instellingen op zoek naar effectievere manieren om hun gevoelige informatie te beschermen en de integriteit van hun data te waarborgen. Hoewel er diverse technologieën zijn die daarvoor uitkomst kunnen bieden, dringt het besef door dat de mens zelf hiervoor het meest effectieve instrument is. Dit besef brengt verandering in de overwegend negatieve perceptie van hacker.



Ethische hackers worden gezien als de nieuwe helden. Zij bieden inzicht in de zwakke plekken van de securitystrategie. Dit biedt waardevolle informatie voor verbetering. Maar als organisaties hackers om hulp vragen, rijst vanzelfsprekend de vraag wat precies een goede hacker is.

Profiel van een hacker

Eerlijk gezegd is het niet bijster moeilijk om systemen te hacken. Hackers zijn overduidelijk in het voordeel. De organisaties waarop zij hun pijlen richten, moeten elke tool, elk systeem en elke interactie veilig zien te houden. Een hacker daarentegen hoeft slechts één gat in de beveiliging te vinden of slechts één werknemer te vinden die op een link in een phishing-mail klikt. Technologie stelt mensen in staat om een goede hacker te worden, maar dat maakt ze nog geen uitmuntende hacker. De beste hackers hebben vier belangrijke karaktertrekken: ze zijn sociaal intelligent, nieuwsgierig, in staat om zich aan te passen en gemotiveerd.

Nieuwsgierigheid

Uitmuntende hackers zijn van nature nieuwsgierig. Ze vragen zich voortdurend af waarom een systeem op een bepaalde manier fungeert, hoe een organisatie te werk gaat, wat de verantwoordelijkheden van het slachtoffer zijn of hoe hij als persoon in elkaar steekt.
Ze willen het naadje van de kous weten van de technologie of persoon in kwestie. Als hackers hun aannames niet uit nieuwsgierigheid toetsen, is dat een garantie voor mislukking, en erger nog, een garantie om in de kraag te worden gevat.

Sociale intelligentie

Doorsnee hackers voeren aanvallen uit op technologie. Slimme hackers richten hun pijlen op mensen. En uitmuntende hackers weten precies wanneer ze een van beide moeten doen. Hackers moeten even nieuwsgierig zijn naar mensen als naar technologie, want steeds opnieuw blijkt dat mensen de zwakste schakel in de beveiliging vormen. Zo blijkt uit de Breach Level Index dat vorig jaar bij 59 procent van alle datalekken sprake was van identiteitsdiefstal. Uitmuntende hackers hebben oog voor deze zwakke schakel en proberen daarom het psychologische profiel van hun doelwit te doorgronden. Door inzicht te verwerven in de manier waarop het slachtoffer denkt en te werk gaat, kan een hacker kwetsbaarheden identificeren om misbruik van te maken.

Aanpassingsvermogen

Om met de woorden van George Santayana te spreken: 'Zij die zich het verleden niet kunnen herinneren, zijn gedoemd om het te herhalen.' Om succesvol te zijn, moeten hackers leren van hun successen en mislukkingen, en zeker ook van die van andere hackers. En daar gaat het nog al eens mis. Zo overschatten hackers nog geregeld hun vermogen om onopgemerkt te blijven. Ze moeten hun tactieken, technieken en procedures dus constant aanpassen om hun doelstellingen te realiseren.

Gemotiveerd

De hackers die normaliter de pers halen, zijn de hackers met kwaadaardige bedoelingen. Zij zijn uit op financieel gewin, proberen de politieke situatie te beïnvloeden of willen simpelweg het slachtoffer in verlegenheid brengen. We hebben nu hackers nodig die bereid zijn om mensen en organisaties te beschermen die een potentieel doelwit vormen. Hackers met een sterk moreel besef die een hoger doel nastreven. Hackers die gevoelige informatie veilig willen houden in plaats van zaken te ontwrichten.

Uitmuntende ethische hackers

Er bestaat geen twijfel over dat deze tijd vraagt om uitmuntende ethische hackers als aanvulling op de bestaande securitystrategie om de veiligheid en integriteit van data beschermen. Ik kijk uit naar de eerste vacatures en wervende teksten. Zie je het ook al voor je? Gezocht: hackers in dienst van de samenleving.

***Geschreven door: Dirk Geeraerts**, identity en data protection expert bij Gemalto, helpt organisaties bij het implementeren van data security oplossingen.*


EUROFORUM
Volledig op de hoogte van Data & Privacy
Euroforum organiseert diverse opleidingen en congressen met betrekking tot Data & Privacy.
Bekijk het complete aanbod