EYE on Finance

2019 ▸ NUMMER 2

AVG, een jaar later

▸ INTERVIEW ◂

"Je kunt de AVG niet in een spreadsheet managen"
Etienne de Cooker - Univé

▸ THEMA-ARTIKEL ◂

"We kantelen van voorlichting naar handhaving"
Aleid Wolfsen - Autoriteit Persoonsgegevens

▸ ROUND TABLE ◂

Een jaar na dato is de AVG niet langer voer voor juristen alleen
Round table met Jeffrey Bholasing – ING
Duco Tuinenburg - NN Group
Saskia Vermeer-de Jongh - HVG Law

EY
Building a better working world

EYE on Finance
is een periodieke uitgave van Ernst & Young Accountants LLP voor relaties in de financiële sector.

Contact
Ernst & Young Accountants LLP
T.a.v. EY Brand, Marketing and Communications
postbus 2295
3000 CG Rotterdam
Tel. 088 407 10 00
E-mail: info@nl.ey.com
Internet: ey.com/nl

Redactie EY
Berna van den Berg,
Yvette Brus,
Jennifer van Eekelen,
Jeroen van der Kroft,
Saskia Vermeer-de Jongh,
Marc Welters.

Met medewerking van
Dirk van der Lit en Nart Wielaard

Ontwerp & vormgeving
BVH Identity Driven Thinking

Drukwerk
Gianotten Printed Media, Tilburg

Disclaimer
EY kan geen aansprakelijkheid aanvaarden voor de gevolgen van activiteiten die worden ondernomen op basis van informatie in deze uitgave. Dit magazine, de inhoud en de vormgeving ervan, zijn eigendom van Ernst & Young Accountants LLP. Alle rechten worden voorbehouden. Niets van deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, openbaar gemaakt, of voor al dan niet commerciële doeleinden worden gebruikt, in enigerlei vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier, zonder schriftelijke toestemming van Ernst & Young Accountants LLP.

Eye on Finance digitaal ontvangen
Eye on Finance is ook digitaal beschikbaar op onze website ey.nl/eyeonfinance. In het kader van duurzaamheid streven wij ernaar om zo min mogelijk gedrukte exemplaren te verspreiden.

Wilt u dit magazine liever digitaal ontvangen, stuur dan een e-mail naar: marion.van.dam@nl.ey.com

Uitschrijven
Wilt u dit magazine niet meer ontvangen? Of wilt u helemaal geen EY-marketing communicatie meer ontvangen? Mail dit dan naar: gdpr.consent@nl.ey.com

IN

HOUD

Saskia Vermeer - de Jongh
Partner bij HVG Law
T +31 (0)6 29 08 38 50
saskia.de.jongh@hvglaw.nl

Defensieve stellingen rondom privacy zijn gelukkig verlaten

Ruim een jaar na inwerkingtreding van de privacywetgeving AVG maken we in deze editie van Eye on Finance de balans op. Het was begin 2018 toen organisaties de dag van 25 mei massaal met dikke viltstiften in hun agenda's markeerden. Actie was geboden, want de nieuwe wetgeving was (en is) streng. Zorg ervoor dat je compliant bent, luidde het mantra, want anders kun je hoge boetes tegemoet zien. Die boetes bleven kort na 25 mei echter uit. Sterker nog: de Autoriteit Persoonsgegevens kwam helemaal niet aan handhaving toe. Ook ondersteuning van bedrijven en instellingen met praktische richtlijnen bleef uit. Daarop ebde de belangstelling voor de privacywetgeving snel weg. De hevige opwinding voorafgaand aan de magische 25 mei maakte plaats voor een oorverdovende stilte rond AVG in de zomer van 2018.

Toen iedereen weer terug was van vakantie brachten veel organisaties in kaart welke privacyprogramma's in werking waren gezet. Sindsdien is daarbij een belangrijke kentering waarneembaar. De defensieve, op compliance gerichte aanpak heeft plaats gemaakt voor een meer open houding rond *data ethics*. Organisaties zijn het privacyvraagstuk veel meer gaan benaderen tegen de achtergrond van gewenste *customer journeys* en de rol van data daarin. Wat mij betreft is het een bijzonder positieve ontwikkeling dat organisaties de intrinsieke motivatie voelen om de waarde van data te benutten en tegelijkertijd begrijpen dat daarvoor spelregels gelden.

Thema's als *data retention, vendor management* en *data governance* staan inmiddels bij veel organisaties hoog op de agenda. Met name ook in de financiële sector, waar traditiegetrouw heel veel data voorhanden is. Mede als gevolg van de AVG, maar ook naar aanleiding van de nog in werking te treden ePrivacy Verordening zoeken financiële organisaties naar een balans om binnen de wettelijke kaders zo goed en efficiënt mogelijk hun klanten te bedienen. Daarbij wordt zoveel mogelijk gebruik gemaakt van gegenereerde data voor een betere klantervaring. Dat de nieuwe generatie klanten daar actief om vraagt, helpt natuurlijk ook. Gewend als de financiële sector is aan strenge regulering, is zij naar mijn mening bij uitstek gepositioneerd om binnen de kaders van de privacywetgeving een succesvolle datastrategie uit te stippelen.

Op korte termijn zal blijken hoe de Autoriteit Persoonsgegevens, die heeft aangegeven dat zij in 2018 veertien onderzoeken is gestart, de AVG zal gaan handhaven. Belangrijk daarin zijn de toezichtthema's en boetebeleidsregels die de AP recentelijk heeft gepubliceerd.
Kijkend naar de toekomst is misschien wel de belangrijkste vraag hoe lang onze privacywetgeving *technology proof* zal blijken te zijn. De introductie van de AVG was de eerste herziening van privacywetgeving in decennia. Zo lang zal een volgende update naar mijn stellige overtuiging echt niet op zich laten wachten.

Ik wens u veel leesplezier met deze editie van Eye on Finance en hoop u te inspireren tot a *better working world*. ●

“Netjes omgaan met data schept basis voor vertrouwen”

Data is de brandstof voor elke moderne financiële instelling en goed omgaan met data is de smeerolie voor het vertrouwen. In deze rubriek bevroeg Jeroen van der Kroft, associate partner bij EY de CEO van Knab Bank en Aegon Bank Eric Rutten hierover. “Transparantie over wat we doen met data neemt bij ons een strategische plek in en we bouwen continu aan een organisatiecultuur waarin dat volkomen vanzelfsprekend is en waarbij de board een voorbeeldfunctie heeft.”

”In mijn ogen bracht de AVG minder nieuws dan soms wordt gedacht. De maatschappelijke digitalisering ging de afgelopen decennia heel hard en daarmee werd het ook steeds belangrijker om op een verantwoorde manier om te gaan met persoonlijke data. In die zin is de AVG dan vooral een bevestiging van die ontwikkeling. En hier en daar ook een wake up call.

Vooral voor financiële instellingen is data zeer interessant. Aan de hand van

> “De uitdaging is om niet te verzanden in gebruiks-voorwaarden en enorme boekwerken

data kunnen we als bank immers veel te weten komen over onze klanten en de gevoeligheid van die data ligt een stuk hoger dan bij veel andere bedrijven. Bovendien speelt er in onze sector een dilemma. We willen enerzijds restrictief zijn in de omgang met data. Simpelweg omdat klanten dat van ons verwachten. Anderzijds hebben we echter ook een poortwachtersfunctie om partijen met kwade bedoelingen in kaart te brengen en dat vergt juist wel veel data.

Vertrouwen is en blijft het allerbelangrijkste voor financiële instellingen. Lang geleden bouwde je aan dat vertrouwen met dikke kluisdeuren, nu gaat het er (ook) om dat je zorgvuldig met data omgaat. De AVG biedt daar wettelijke normen voor. Minstens even belangrijk als die normen is wat onze klanten zelf willen. Daarom luisteren we in onze klantcommunities ook heel goed naar wat zij ons hierover vertellen.

Een van de zaken die we goed op orde moeten hebben is transparantie over wat we doen met data. De uitdaging daarbij is om niet te verzanden in gebruiksvoorwaarden en enorme boekwerken. We moeten zoveel mogelijk eenvoud bieden, want daaraan ontleent de klant het vertrouwen. Daarbij gaat het niet alleen om informeren maar ook de klant nadrukkelijk zelf aan de knoppen te zetten. De klant moet eenvoudig het beheer krijgen over waar hij wel en geen toestemming voor geeft. Tot slot vinden we ook actieve voorlichting belangrijk zodat klanten goed beslagen ten ijs komen en bijvoorbeeld de gevaren van phishing onderkennen.

Als bestuurder moet ik erop toezien dat de organisatie permanent aandacht blijft geven aan het verantwoord omgaan met data. Dat betekent onder andere dat je intern experts mobiliseert om je organisatie scherp te houden, zeker omdat technologie zich snel blijft ontwikkelen en daarmee nieuwe vraagstukken op tafel legt. Denk bijvoorbeeld aan de steeds grotere rol die geautomatiseerde controles spelen.

Het thema heeft ook in onze strategie een sleutelpositie gekregen: digitale technologie speelt daarin de hoofdrol en om die strategie succesvol uit te voeren moet je verantwoord omgaan met data. Dat vereist dat dit thema een vaste en natuurlijke plek moet hebben in alles wat je doet, in je *way of working* en in je cultuur. Doordat we bij het ontwikkelen van nieuwe producten en diensten in agile teams werken is dat goed mogelijk. Een van de kernpunten van agile is immers dat je met een multidisciplinair team werkt, met daarin ook expertise over een verantwoorde omgang met data.

> “Betrek je klant bij het beheer van zijn data, het is zijn privacy, niet het jouwe

Ook in de afstemming met derde partijen speelt verantwoorde omgang met data een grote rol. Als bank opereer je allang niet meer standalone en werk je steeds meer samen in een ecosysteem met tal van partners waardoor third party risk management steeds belangrijker wordt. Dat betekent dat je de normen en waarden van je organisatie moet doorgeven en je er ook actief op toeziet dat je partners goed met de data van onze klanten omgaan.

Commissarissen houden ons ook scherp op het AVG dossier. Niet omdat er aanzienlijke boetes kunnen worden opgelegd of omdat bestuurders aansprakelijk gesteld kunnen worden. Dat speelt eigenlijk geen rol in de discussies erover. Veel belangrijker: het gaat om het vertrouwen en daarmee om het bestaansrecht van een bank. We informeren commissarissen dan ook actief over hoe we omgaan met privacy thema’s en hun kritische vragen leiden tot waardevolle discussies.”

‘We kantelen van voorlichting naar handhaving’

Volgens Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens (AP), zitten we in overdrachtelijke zin nog maar in de middeleeuwen van een enorme maatschappelijke digitalisering. Juist in zo’n snelle technologische ontwikkeling is er eigenlijk geen andere optie dan het hanteren van open normen voor privacy. In gesprek met Nicolette Opdam (partner HVG Law) geeft hij zijn visie op wat dat betekent voor de handhaving van de AVG.

Van rechter naar Tweede Kamerlid naar burgemeester naar voorzitter van de Autoriteit Persoonsgegevens. Wolfsen heeft in zijn loopbaan in tal van hoedanigheden middenin het omgaan met recht gestaan en heeft er zichtbaar plezier in om nu met ‘zijn’ AP toezicht te houden op de bescherming van de privacy van burgers. Ook al omdat het volgens hem gaat om de moeder van alle grondrechten. Volgens de redenering dat bijvoorbeeld vrijheid van godsdienst staat of valt met privacy: “Het is heel bijzonder dat we voor dit grondrecht met de invoering van de AVG nu een eigen handhaving hebben, dat is voor geen enkel ander grondrecht het geval. We mogen daar ook best trots op zijn. Ik vind het bijvoorbeeld mooi om te zien hoe de aanvankelijke scepsis in de Verenigde Staten nu omslaat naar interesse over hoe we dat in Europa regelen.”

Terugkijkend op de implementatie van de AVG, wat is u opgevallen hier in Nederland?

“De enorme bewustwording. Nederlanders beseffen de waarde van privacy, en uit enquêtes blijkt ook dat de Nederlandse burger op dat punt hoger scoort dan alle andere burgers in andere Europese landen. Wellicht heeft dat ook te maken met het feit dat we digitaal op veel fronten in de kopgroep zitten, en dat privacy juist door digitalisering een steeds relevanter thema wordt. Dat is bijvoorbeeld te zien in de vergaande digitalisering van financiële diensten waarin Nederland echt een koploper is. Je bankrekening kan heel veel vertellen over jou, van je politieke kleur tot je seksuele voorkeur. En dus is het zaak om daar zorgvuldig mee om te gaan. Kleine anekdote: ik kwam onlangs thuis van een tweedaagse reis naar Brussel en moest een euro betalen voor de stalling van mijn fiets op het station in Utrecht. Toen ik thuis kwam had mijn vrouw de piepers al bijna klaar, terwijl ik haar geen bericht had gestuurd dat ik onderweg was. Wat bleek: ze had op de bankapp net gezien dat ik die euro had betaald en wist dat ik er aankwam.”

> “Het gaat om de open normen invullen naar de geest van de wet

Toen de AVG kwam gaf de AP een inkijkje in de prioriteiten in het toezicht op de naleving. De financiële sector stond niet tussen die prioriteiten. Wat kunnen we daaruit afleiden?

“We hebben ons toezicht tweeledig ingericht: enerzijds op basis van de klachten die we binnenkrijgen, en anderzijds op basis van maatschappelijke zorgen over de veiligheid en de privacy van gegevens. We moeten wel keuzes maken over waar we meer of minder werk van maken omdat we met 170 FTE’s niet alles kunnen doen. We besteden momenteel veel capaciteit in de zorg en bij overheden. Ten aanzien van de financiële sector ben ik overigens positief gestemd.

Financiële instellingen lijken het thema goed opgepakt te hebben en hebben bovendien ervaring met toezichthouders op andere domeinen. Dat helpt waarschijnlijk ook."

> Het is eenvoudiger om te zeggen wat lelijk is, dan wat mooi is

Daarover gesproken: is er veel overleg met andere toezichthouders?

"We hebben periodiek overleg met DNB en AFM. Het is heel waardevol, niet alleen om signalen maar ook beelden uit te wisselen. We moeten er ook voor zorgen dat er geen overlap ontstaat in het toezicht. Een deel van de privacytaken leek in eerste instantie bij DNB terecht te komen, maar dat is nu toch ondergebracht bij de AP. Ik vind dat een goede zaak omdat wij – in tegenstelling tot DNB – een Europees mechanisme hebben met alle andere privacytoezichthouders om toe te zien."

De invoering van wetgeving zoals de AVG leidt vrijwel onvermijdelijk tot lastige dilemma's. De sector zoekt in de spreekwoordelijke grijze gebieden dan ook naar houvast en kijkt daarvoor naar de AP. Kunt u die 'guidance' geven?

"Er is sprake van open normen in de AVG en dan is het heel logisch dat die dilemma's er zijn. Het is maar goed ook dat we met open normen werken want het gaat om een heel breed domein waar de ontwikkelingen razendsnel gaan en waar een rule based benadering snel door de ontwikkelingen in de praktijk zou worden ingehaald. We staan voor mijn gevoel nog maar in de middeleeuwen als het gaat om de maatschappelijke digitale transformatie, en er komt dus nog heel veel op ons af. Bij de bescherming van de privacy moeten we kunnen meeademen met de golven van de nieuwe technologie. Open normen maken dat mogelijk. Toezicht uitoefenen met open normen in de hand betekent dat je ook kijkt naar de geestesgesteldheid waarmee organisaties de wet naleven en omgaan met persoonlijke gegevens. Neem bijvoorbeeld het thema privacy by design, waar sprake is van zo'n open norm. Organisaties moeten bij de ontwikkeling van nieuwe systemen of applicaties vanaf het begin de privacy de juiste plek geven in de software. Dat is een prachtig principe en waar wij als toezichthouder dan vooral naar kijken is of er bij de opdrachtverstrekking serieuze aandacht is voor privacy. Overigens is dat ook in andere domeinen van het recht heel gebruikelijk. In het civiele recht kennen we het begrip goed huisvader in dat verband. De AVG kent bijvoorbeeld met een beginsel als 'passend' een soortgelijk basisprincipe."

Toch zoeken veel financiële instellingen meer zekerheid over de twijfelgevallen. Ze willen weten waar ze aan toe zijn. Begrijpt u dat?

"Ik begrijp dat heel goed en we spelen daar waar mogelijk ook op diverse manieren op in. Toevallig hadden we vanmorgen nog een symposium waar maar liefst 700 functionarissen gegevensbescherming op af kwamen. Dat is een uitstekende gelegenheid om de dialoog te voeren. Zij zijn feitelijk de vooruitgeschoven post in het toezicht. Verder doen we veel via branche- en koepelorganisaties waar we dan ook duiding kunnen geven over bepaalde zaken en we hebben wat Q&A's ontwikkeld rondom het begrip 'toestemming geven'. En het komende jaar zal er zeker meer casuïstiek ontstaan waar instellingen zich op kunnen baseren om vragen in het grijze gebied goed te beantwoorden. Het is een beetje zoals met schoonheid, het is vaak eenvoudig om aan te geven wat lelijk is, wat wel of niet mooi is, ligt lastiger. Het punt is dat we als toezichthouder vooral kunnen zeggen wat lelijk is, en niet wat mooi is."

Ik hoor de financiële sector niet specifiek voorbij komen als een sector die speciale aandacht behoeft... Heeft u een specifieke observatie over die sector?

"Naast het feit dat gegevens bij banken en verzekeraars vaak zeer persoonlijk zijn, zijn we nu vooral betrokken bij het intermediairskanaal. In deze sector is niet altijd voldoende kennis over hoe je om moet gaan met het geven van toestemming voor het gebruik van gegevens. En over de vraag of je – volgens de definitie van de AVG – verwerker of verwerkingsverantwoordelijke bent."

> Privacy is de moeder van alle grondrechten

Wat kunnen we komend jaar verwachten van de AP?

"We hebben afgelopen jaar heel veel gedaan aan voorlichting. Het komende jaar kantelen we naar handhaving. Er loopt een aantal onderzoeken op dit moment waarbij ook zaken die de financiële sector raken worden meegenomen."

Transparantie en toegangs-beveiliging wegen zwaar bij internationale handhaving van privacywetgeving

Transparantie, toegangsbeveiliging en de vereisten voor het verkrijgen van geldige toestemming voor de verwerking van persoonsgegevens. Dat zijn thema's waar internationale toezichthouders op privacywetgeving zich vooral op blijken te richten.

Volgens Wout Olieslagers, privacydeskundige bij HVG Law, zijn er het afgelopen jaar ongeveer honderd GDPR-boetes opgelegd, in omvang variërend van een paar duizend tot vijftig miljoen euro. Die laatste sanctie werd door de Franse toezichthouders opgelegd aan Google, vanwege het gebrek aan transparantie over de wijze waarop het bedrijf met persoonsgegevens van klanten omgaat.
Deze zaak laat volgens Olieslagers zien hoe belangrijk die transparantie is voor toezichthouders: "Google had namelijk wel alle vereiste informatie online beschikbaar, maar in versnipperde vorm. Belangrijk is om die informatie op één plek beschikbaar te hebben volgens het zogenaamde 'one-click away' vereiste. Dat de boete voor Google zo hoog uitviel is volgens hem dan ook goed verklaarbaar: "De autoriteiten letten er bij het opleggen van een boete onder andere op dat deze daadwerkelijk impact heeft op de organisatie." Een andere boete over ditzelfde onderwerp, informatievoorziening, is opgelegd aan de Poolse marketingorganisatie Bisnode.
Het bedrijf had niet van al haar klanten e-mailadressen terwijl het wel over de postadressen beschikte. Bisnode koos ervoor om de klanten van wie het bedrijf alleen het postadres had niet een brief te sturen, maar voor die groep bedoelde informatie alleen op de website te plaatsen. De Poolse autoriteit oordeelde dat Bisnode daarmee onvoldoende inspanning had verricht om iedereen te informeren. De boete bedroeg € 220.000.

Twijfelachtige eer

Toegangsbeveiliging van IT-systemen is volgens Olieslagers een ander focuspunt voor toezichthouders. Een Portugees ziekenhuis komt de twijfelachtige eer toe dat zij op dit gebied de allereerste GDPR-boete heeft moeten incasseren. In het ziekenhuis hadden ongeveer duizend mensen toegang tot patiëntgegevens, terwijl er nog geen driehonderd artsen werken. Boete: € 400.000. Ook in Noorwegen heeft de autoriteit een boete opgelegd, in dat geval aan een scholengemeenschap, voor het onvoldoende beveiligen van IT-systemen. Daardoor konden alle medewerkers van de scholengemeenschap inloggen en persoonsgegevens van scholieren raadplegen. De hoogte van de boete was in dit geval circa € 170.000.
Een ander belangrijk aandachtsgebied betreft de manier waarop bedrijven en instellingen klanten om toestemming vragen voor het verwerken van persoonsgegevens. Olieslagers: "Dat moet zo specifiek mogelijk zijn voor de activiteit die de organisatie verricht. Je kunt dus niet één keer toestemming vragen en vervolgens maar je gang gaan. De klant moet zicht hebben op mogelijke risico's die hij of zij loopt."

Wout Olieslagers
Advocaat bij HVG Law
T +31 (0)6 52 46 56 93
E wout.olieslagers@hvglaw.nl

Nederlandse pijnpunten belicht in internationaal privacy-onderzoek

In samenwerking met de *International Association of Privacy Professionals* (IAPP) brengt EY eind september het vijfde *Annual Privacy Governance Report* uit. De aandacht voor de Europese introductie van de *General Data Protection Regulation* zal in vergelijking met een jaar eerder flink toenemen. "Gedurende het veldwerk hebben we dan ook uitvoerig gevraagd naar de ervaringen en prestaties van Europese bedrijven en instellingen op privacygebied," zegt Bernadette Wesdorp, privacy expert bij EY. "Organisaties zijn op zoek naar houvast. Ze willen nadrukkelijk weten hoe ze het doen ten opzichte van de benchmark. Bijvoorbeeld als het gaat om budgetten, programmaprioriteiten en de inzet van medewerkers en tools."

Ingrijpende exercitie

Wesdorp verwacht dat het nieuwe onderzoek duidelijkheid verschaft voor wat in Nederland als lastig wordt ervaren. "Allereerst speelt dat rondom het recht op inzage en verwijdering van persoonsgegevens. Waar komen zulke verzoeken van klanten binnen? Hoeveel zijn het er? Kun je ze handmatig verwerken of is dat buitengewoon inefficiënt? En welk type verzoeken is lastig om binnen de daarvoor vastgestelde termijn van dertig dagen te behandelen?"

Een tweede punt waar de markt tegen aanhikt, is volgens Wesdorp het inrichten van een register van processen waarin persoonsgegevens worden gebruikt. "Zo'n overzicht is het eerste waar de toezichthouder om vraagt als die op de stoep staat. Het register moet compleet en actueel zijn. Organisaties vinden dat moeilijk omdat het niet over één afdeling gaat, maar over de totale organisatie. Dan praat je over een ingrijpende exercitie, die men vanzelfsprekend financieel beheersbaar wil houden. Zeker als je het register continu *up to date* moet hebben."

Bernadette Wesdorp
Manager EY Financial Services Advisory
T +31 (0)6 21 25 27 53
bernadette.wesdorp@nl.ey.com

Relaties delen ervaringen op GDPR Anniversary Event

Zorg in ieder geval voor een control framework en wijs in de organisatie privacy champions aan. Dat waren twee belangrijke aanbevelingen op basis van behandelde casussen tijdens het door EY georganiseerde GDPR Anniversary Event, eind mei in Amsterdam.

Tijdens het evenement deelden ongeveer zestig klanten en relaties van EY hun ervaringen met de Europese privacywetgeving van het afgelopen jaar. Met elkaar wisselden zij van gedachten over thema's als data management, governance, third party risk management, legal & compliance en security & privacy. Onderdeel van de bijeenkomst was ook de behandeling van twee casussen in vier verschillende teams. Centraal stonden twee vragen: hoe rol je een wereldwijd programma uit in een decentrale organisatie, en op welke manier kun je aantonen dat de getroffen maatregelen in de praktijk ook echt werken?

Behoorlijk eensgezind

Dat de teamleden aan de afzonderlijke sessies uiteindelijk behoorlijk eensgezind in de door hen aanbevolen aanpak waren, bewees dat zij al de nodige praktijkervaring in hun bagage hebben. In eerste instantie pleitten de deelnemers voor een control framework. Desgewenst uitsluitend rondom privacy of als onderdeel van een groter (integrated) control framework. Daarnaast benadrukten de aanwezigen het belang van goede communicatie over doelstellingen, de noodzaak van onderhoud door middel van training en de aanwijzing van decentrale privacy champions die het bewustzijn over het privacyvraagstuk in de decentrale organisatie levend houden. Ook board involvement en een stapsgewijze aanpak ('land na land' en 'bottom up') werden genoemd als succesfactoren voor een geslaagde wereldwijde implementatie. Voor het bewijs dat de getroffen maatregelen aantoonbaar werken, pleitten de deelnemers voor een governancestructuur met op het control framework gebaseerde rapportagelijnen. Daarnaast gingen er meerdere stemmen op voor het auditen van het framework en anderen noemden ook certificering als mogelijkheid om de buitenwereld te laten zien dat de organisatie de privacyverplichtingen serieus neemt. Aangezien er nog geen best practice is, zullen de varianten nog wel even naast elkaar bestaan.

‘Je kunt de AVG niet in een spreadsheet managen’

Je kunt wet- en regelgeving zien als een ‘moetje’. Je kunt het ook positiever benaderen door, naast te voldoen aan alle eisen, ook te redeneren vanuit de hogere doelstelling van de wet. Dat levert meer op. In gesprek met Jennifer van Eekelen van EY, laat directeur Etienne de Cooker van Univé zien voor het laatste te kiezen en de AVG vooral in te zetten voor een organisatiecultuur waarin je elkaar actief aanspreekt op privacy.

> “In het begin was het grijze gebied vrij groot. Dat verkleinen we nu steeds verder.

In het jaar nadat de AVG formeel van toepassing werd, heeft Univé te maken gehad met 19 klanten die verzochten om inzage in hun gegevens, en waren er 31 verzoeken om gegevens te verwijderen. Op een bestand met ongeveer 1,5 miljoen klanten is dat haast verwaarloosbaar. De Cooker is niet verrast, want het past in zijn verwachtingspatroon:

‘Univé is een bijzondere organisatie met een hoge klanttevredenheid en -vertrouwen. Dat heeft alles te maken met onze historie als coöperatie waarin leden altijd een belangrijke rol hebben gespeeld en met de zichtbaarheid van ons merk in het straatbeeld, met zo’n 110 winkels. We staan bekend als een laagdrempelige organisatie die luistert naar haar klanten, onder meer in klantenpanels. Onze klanten vertrouwen er dan ook terecht op dat wij goed met hun gegevens omgaan.’

Klinkt goed, maar elke verzekeraar zal zeggen dat ze goed voor hun klanten zorgen. Wat maakt Univé anders?
'Jaren geleden ging ik voor het eerst naar een regionale ledenbijeenkomst in Emmen. Bleken daar 1500 mensen op af te komen. De betrokkenheid is erg hoog, en we doen ook echt wat met de meningen en ervaringen van onze klanten. Een van de mooiste anekdotes gaat over een klant die ontdekte dat er kleine afrondingsverschillen ontstonden op de factuur. Ze maakte daar serieus werk van ook al ging het over centen. Daar kun je je schouders over ophalen, maar dat doen we hier niet. We besloten de klacht serieus te nemen en het systeem aan te passen, in de wetenschap dat zo'n systeemwijziging toch ook geld kost. Ook bij de verzoeken tot verwijdering laten we zien dat we de klant serieus nemen. Deze verzoeken komen vaak voort uit ongenoegen, niet gerelateerd aan privacy. Door te bellen met deze klanten kun je veel over hun verzoek leren.'

> "Ik wil niet 1 speler in het veld die door 10 stafleden wordt geadviseerd

Een organisatie als Univé ontwikkelt zich voortdurend. Er komen producten bij, er worden nieuwe systemen ontwikkeld. Hoe zorg je in die dynamiek dat je blijft voldoen aan de eisen van AVG?
'In dergelijke gevallen voeren we dan uiteraard opnieuw Privacy Impact Assessments uit. De implementatie van de AVG is nu eenmaal geen eenmalige vingeroefening. Juist daarom stimuleren we breed eigenaarschap.
Alle regionale Univé's hebben een eigen Functionaris Gegegevensbescherming (FG) voor het toezicht en die werken nadrukkelijk samen met mensen in het veld. En wij doen dat bij Univé Schade uiteraard ook. Ik denk dat binnen Univé inmiddels zeker 30 mensen veel kennis hebben over de AVG en we blijven voor alle medewerkers het thema ook aandacht geven in e-learnings. We hebben een privacy office en privacy teams. Wat misschien wel het allerbelangrijkste is: het is volstrekt geaccepteerd dat je in meetings wijst op de privacyaspecten als er nieuwe plannen op tafel komen. En dat is dan niet alleen een verantwoordelijkheid voor de FG. In mijn ogen is breed eigenaarschap de enige werkbare optie. Meer algemeen: organisaties als de onze hebben te maken met een overvloed aan wet- en regelgeving. We moeten ervoor waken niet alles naar stafafdelingen weg te delegeren. Want dan is de balans ver te zoeken en staat er straks één speler in het veld die langs de lijn door tien anderen wordt geadviseerd en gecontroleerd.'

Wat zijn lastige dilemma's in de uitvoering?
'We constateerden bij de start van het project al dat de AVG eigenlijk een groot dilemma blootlegt. Enerzijds willen we veel van onze klanten weten. Want hoe meer we weten, hoe beter we ze van dienst kunnen zijn. Anderzijds willen we ook dat klanten erop kunnen vertrouwen dat er geen misbruik van hun data kan worden gemaakt en dat die dus veilig zijn bij ons. Dat spanningsveld zie je hier en daar ook concreet terug in botsende casussen. Dat kan ook voortvloeien uit wetgeving overig-

ens. De AVG staat voor privacy en daarbij hoort terughoudendheid bij het vastleggen van identificatiebewijzen. Vanuit de sanctiewetgeving – bedoeld om terroristische activiteiten tegen te gaan – is dat juist wel nodig. Dat vereist dus goede communicatie en het maken van keuzes. Overigens is er een groot voordeel van de AVG boven dergelijke meer specialistische wetgeving: de AVG is echt voor alle klanten en medewerkers van toepassing en dus bij iedereen bekend. Dat maakte de implementatie een stuk gemakkelijker. En de doelstelling staat niet ter discussie: iedereen wil dat zijn of haar privacy goed geborgd is.'

> “
> Elkaar aanspreken werkt het beste

Waren er voor Univé nog meer van dergelijke praktische knelpunten?
'Ik denk dat we aanliepen tegen veel zaken waar ook andere verzekeraars mee te maken hebben. Dat we in de branche geen goed concept hebben om dataportabiliteit te regelen bijvoorbeeld. Heel specifiek voor Univé: we bieden FNV-leden kortingen. De AVG is daarin echter heel duidelijk: je mag niet vastleggen dat mensen lid zijn van een vakbond. Dat levert dus een dilemma op, want je wilt de vakbondsleden de korting niet onthouden. De oplossing was in dit geval dat we voortaan registreren dat ze lid zijn van een collectief, maar niet het vakbondslidmaatschap. Het belangrijkste bij dergelijke voorbeelden is dat je kunt beargumenteren waarom je bepaalde keuzes maakt. Aan je klant, aan jezelf en als het zover zou moeten komen ook aan de rechter. Vanuit die gedachte bouwen we aan ons moreel kompas. In het begin hadden we een vrij groot grijs gebied waar we zochten naar houvast. Dat grijze gebied wordt nu steeds kleiner.'

Zoek je voor het oplossen van deze grijze gebieden ook afstemming met de toezichthouder?
'Ik denk eerlijk gezegd niet dat er een spoorboekje te maken valt dat op alle vragen antwoord geeft. Ook de toezichthouder kan dat niet. Waar het om gaat is dat je het bewustzijn, de kennis en de cultuur bevordert waarin de organisatie zelf goed haar afwegingen kan maken. In het begin hebben we ons ook door externen laten uitdagen. Dat helpt om een referentiekader te creëren.'

Zo te horen heeft Univé de governance van persoonsgegevens goed op orde?
'We zijn heel goed op weg, maar je kunt natuurlijk geen garanties geven dat er nooit wat mis gaat. Ik denk dat het zaak is vooral het thema te blijven benoemen en het daarmee levend te houden. Daar ligt ook een belangrijke taak voor ons als directie. Soms zit dat in kleine dingen. Onlangs was ik betrokken bij een sollicitatieprocedure, waarbij cv's van mensen per mail worden verstuurd aan een klein groepje. Dan stuur ik wat later wel een mail rond met de vraag of iedereen die cv's inmiddels heeft verwijderd uit de mailbox. Daarmee probeer ik eraan bij te dragen dat goed omgaan met persoonlijke data gewoon *business as usual* is. De neiging is om dergelijke onderwerpen in een spreadsheet te managen en daarmee te laten zien dat je voldoet aan alle eisen. Maar elkaar aanspreken werkt echt beter.'

Privacy Control Framework een bruikbaar instrument bij privacy audits

De praktijkervaringen van auditors die afgelopen jaar met het Privacy Control Framework (PCF) van de beroepsvereniging van IT-Auditors (NOREA) hebben gewerkt, worden actief gebruikt voor een eerste update van dit normenkader, dat bovendien ook in een Nederlandse versie zal worden gepubliceerd. Voor IT-auditors is het PCF een officiële handreiking bij privacy audits en assuranceopdrachten voor het Privacy Audit Proof keurmerk. Voor AVG-certificering in de betekenis van de wet heeft het nog geen formele status," constateert medeopsteller van het normenkader Ed Ridderbeekx in gesprek met Stijn Giesberts, privacy expert van EY.

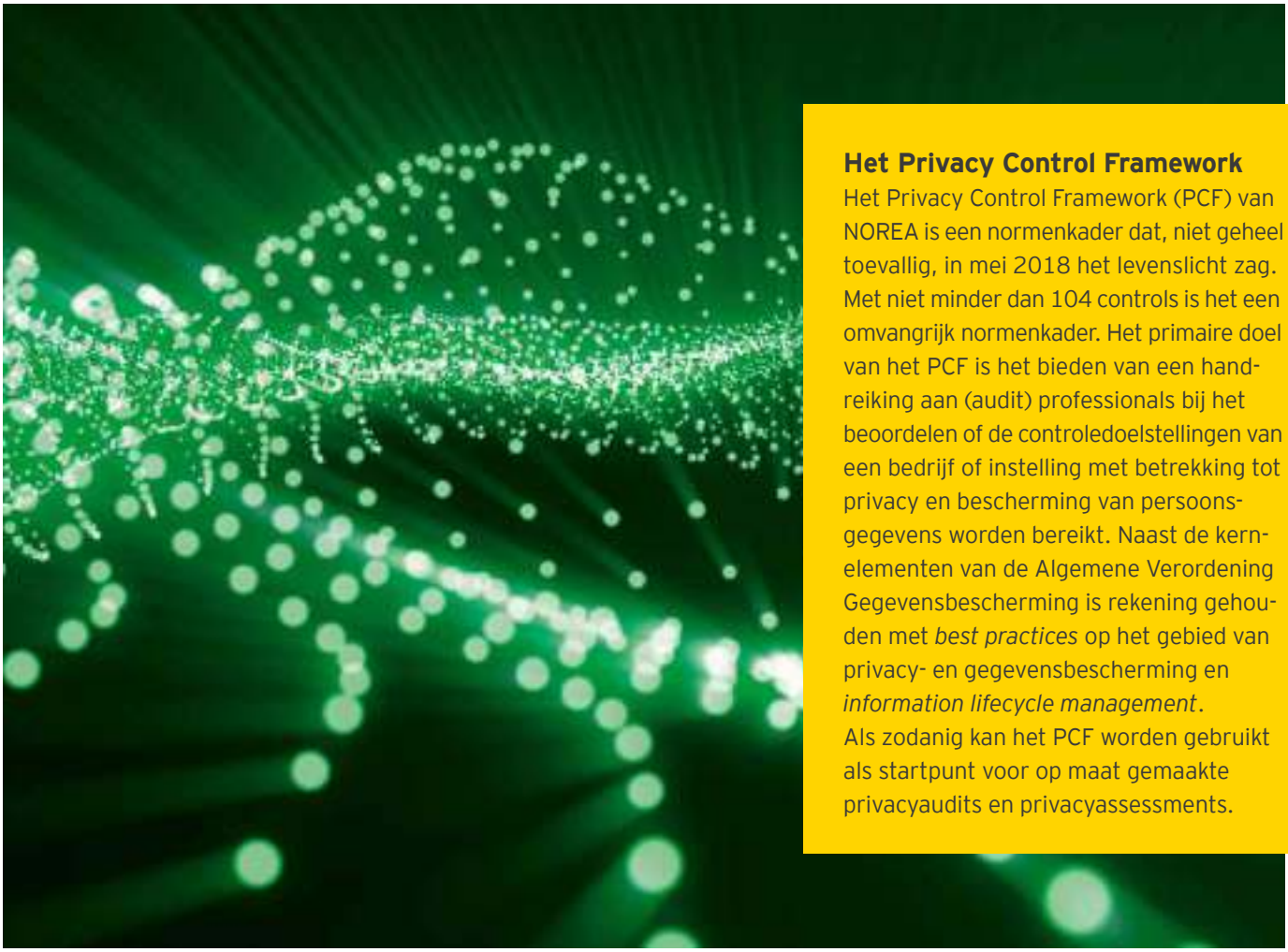
De NOREA houdt zich van oudsher intensief bezig met de ontwikkeling van normen en standaarden voor de beoordeling van IT-beheer. Vanzelfsprekend ondersteunt de vereniging de aangesloten register IT-auditors bij de nieuwe privacywetgeving met behulp van concrete beheersdoelstellingen voor de bescherming van persoonsgegevens en adequate technische en organisatorische beveiligingsmaatregelen. "In de aanloop naar 25 mei 2018 is daar door de Kennisgroep Privacy van NOREA hard aan gewerkt," zegt Ed Ridderbeekx die nauw betrokken was bij de opstelling van het Privacy Control Framework.

Lastige terminologie

Ridderbeekx benadrukt dat dit framework *from scratch* is gebouwd. "We namen de AVG en een referaat van een aantal collega's als vertrekpunt en hebben tegelijk uitvoerig gekeken naar concepten als *privacy by design* en *privacy by default*. Dan heb je het over tamelijk ingewikkelde concepten die niet altijd op dezelfde manier worden geïnterpreteerd. Het is intrinsiek lastige terminologie. Als ik bij bedrijven op bezoek ben en het gesprek komt op *privacy by design*, dan adviseer ik altijd: houd in ieder geval bij de ontwikkeling van nieuwe producten of diensten rekening met alle mogelijke privacy issues. En vooral: documenteer dat ook. Zo maak je het hanteerbaar. Veel hangt af van de aard en de omvang van de organisatie waar je mee te maken hebt. Met het normenkader van NOREA kunnen we echter niet alles regelen. Het professionele oordeel van de auditor blijft uiteraard nodig."

> "
>
> *Privacy by design* is intrinsiek lastige terminologie

Ruim een jaar na de introductie van het PCF zijn er zowel in Nederland als daarbuiten tal van andere normenkaders gelanceerd. Ridderbeekx betwijfelt of hij een volledig beeld daarvan heeft. "Maar," zegt hij, "als ik er dan toch een moet uitlichten, dan noem ik het Luxemburgse CARPA framework. Dat normenkader is ontwikkeld door de Luxemburgse toezichthouder, die zich zeer actief opstelt als het gaat om certificering conform de uitgangspunten van de privacywetgeving. Daar kunnen professionele *audit firms* en certificerende instellingen vervolgens mee aan de slag. De Luxemburgse insteek is anders dan de Nederlandse situatie, waar de Autoriteit Persoonsgegevens de ontwikkeling van certificeringsschema's aan de markt over laat."



Het Privacy Control Framework

Het Privacy Control Framework (PCF) van NOREA is een normenkader dat, niet geheel toevallig, in mei 2018 het levenslicht zag. Met niet minder dan 104 controls is het een omvangrijk normenkader. Het primaire doel van het PCF is het bieden van een handreiking aan (audit) professionals bij het beoordelen of de controledoelstellingen van een bedrijf of instelling met betrekking tot privacy en bescherming van persoonsgegevens worden bereikt. Naast de kernelementen van de Algemene Verordening Gegevensbescherming is rekening gehouden met *best practices* op het gebied van privacy- en gegevensbescherming en *information lifecycle management*.
Als zodanig kan het PCF worden gebruikt als startpunt voor op maat gemaakte privacyaudits en privacyassessments.

Autoriteit Persoonsgegevens

Onderdeel van 'de markt' is natuurlijk ook NOREA. Heeft Ridderbeekx niet stiekem gehoopt dat de Autoriteit Persoonsgegevens (AP) geïnteresseerd zou aankloppen voor eventuele samenwerking? "NOREA heeft een goede traditie van overleg met de AP en haar voorganger het College bescherming persoonsgegevens. In het kader van het PCF en de AVG is een aantal keer met de AP gesproken. Ze kennen ons framework en staan positief tegenover de ontwikkeling van zo'n privacy-normenkader, maar dat heeft nog niet geleid tot formeel endorsement van het PCF, bijvoorbeeld als een set van criteria die gebruikt kunnen worden voor wat de AP 'AVG-certificering' noemt. We blijven uiteraard in overleg met de AP."
NOREA heeft volgens Ridderbeekx vooral feedback uit het werkveld opgepikt. "Bij een bijeenkomst met een groep *privacy officers* werd bijvoorbeeld aan de orde gesteld in welke mate de informatiebeveiliging van ISO27001 overlap vertoont met ons PCF. Daarom neemt NOREA in de eerstvolgende update van het framework ook een *mapping* met ISO27001 op. Aan de nieuwe versie wordt momenteel de laatste hand gelegd, de publicatie is deze zomer gepland. Ridderbeekx: "Organisaties die nu met het PCF werken ervaren het in de praktijk als een heel bruikbaar instrument. Wel wordt een Nederlandstalige versie node gemist, en die komt er dan ook."

ISO-richtlijn 27552

Een ander punt van kritiek op het PCF is dat het wel een heel omvangrijk document is. "En dat terwijl we niet eens hebben nagestreefd om een raamwerk te creëren op basis waarvan je volledig compliant bent aan de AVG", stelt Ridderbeekx. "We streefden naar het aanbieden van een referentiekader dat redelijke zekerheid kan geven dat je als organisatie geaccepteerde privacyprincipes toepast en de kernelementen van de AVG daarbij betrekt. In de kern wijzigt het nieuwe PCF dan ook niet, dat zou ik ook niet willen." Andere organisaties zitten ook niet stil. ISO werkt momenteel aan de 27552-standaard, waarmee een privacycomponent wordt toegevoegd aan de bekende informatiebeveiligingsstandaard ISO27001. "Voor organisaties die al ISO27001 gecertificeerd zijn of die ISO27001 gebruiken als kader voor informatiebeveiliging kan dat een hele interessante toevoeging zijn."

Stijn Giesberts
Senior Manager EY Financial Services Advisory
T +31 (0)6 52 46 58 93
stijn.giesberts@nl.ey.com

Verantwoord omgaan met klantgegevens gaat meer over ethiek dan over privacy

Door Tony de Bos

Met de inzet van technologie op het gebied van *data analytics* en *artificial intellgence* (AI) komen financiële instellingen steeds meer over hun klanten aan de weet. Dat kan leiden tot allerlei dilemma's waar bestaande regelgeving geen antwoord op heeft. Daarom moeten instellingen zelf verantwoordelijkheid nemen en beleid op *data ethics* ontwikkelen.

Dankzij de introductie van PSD2 nemen de mogelijkheden om rendement op data te genereren duizelingwekkend snel toe. Aan de hand van betaalgegevens van klanten kunnen instellingen, uiteraard met toestemming van diezelfde klanten, met behulp van data analytics en artifical intelligence (AI) allerlei innovatieve diensten ontwikkelen. Deze nieuwe diensten zullen in de eerste plaats moeten voldoen aan de AVG. Het moet voor de gebruiker duidelijk zijn waarvoor persoonsgegevens worden gebruikt. Als aan die voorwaarde is voldaan, kunnen de *data scientists* aan de slag.

Het arsenaal aan mogelijkheden om data te laten renderen, heeft echter ook een schaduwzijde. De grote hoeveelheden (persoonlijke) data in combinatie met geavanceerde technologie kunnen inzichten bieden die instellingen voor sociale of maatschappelijke dilemma's stellen.

De technologische ontwikkelingen rond het gebruik van data gaan namelijk dermate snel dat wetgeving nooit in staat zal zijn om dat bij te benen. Bedrijven en instellingen zullen zelf verantwoordelijkheid moeten nemen voor de manier waarop ze met data omgaan. Daarmee begeven we ons op het terrein van *data ethics*.

Online casino's

Voor elke financiële instelling, of het nou een fintech of een gevestigde corporate is, is het een geweldige uitdaging om rendement op data te realiseren. Met geavanceerde technologie op het gebied van data analytics en AI kunnen modellen worden gebouwd die in staat zijn om patronen in dataverzamelingen te herkennen. Op basis van die patronen is het mogelijk om betrouwbare uitspraken te doen over toekomstig menselijk gedrag. Bijvoorbeeld dat een bankklant over pakweg twee maanden in ernstige financiële moeilijkheden komt te verkeren. Zelfs als de klant in kwestie toestemming heeft verleend om zijn data te gebruiken, dan nog is het de vraag: wil de klant wel geïnformeerd worden over die toekomstige situatie? Die informatie is immers van een geheel andere orde dan de aanbeveling om de huidige energieleverancier te verruilen voor een concurrent omdat die een goedkoper aanbod heeft.
Nog ingewikkelder wordt het als uit de verkregen data blijkt dat de klant structureel grote bedragen overmaakt aan online casino's. In combinatie met bijvoorbeeld het gegeven dat de rekeninghouder grote betalingsachterstanden bij de woningbouwcorporatie heeft, kan dat wijzen op een ernstige vorm van gokverslaving. Wat moet een financiële instelling met die kennis? De klantrelatie beëindigen? Hulpverleningsinstanties inschakelen? Of, als tevens sprake is van inkomende geldstromen die overduidelijk een verdachte herkomst hebben, de politie bellen?

Morele kompas

Financiële instellingen moeten zich ervan bewust zijn dat ze in de toekomst steeds vaker tegen dilemma's als hierboven geschetst aan zullen lopen. Daarom doen ze er verstandig aan om voor zichzelf te bepalen waar hun grens ligt: wat is wel en niet acceptabel? Situaties die volgens het ontwikkelde beleid als onacceptabel gelden, zullen door alle medewerkers als zodanig herkend moeten worden. Vervolgens kan het gesprek over die situaties plaatsvinden. Niet alleen dient dit ethische bewustzijn binnen de eigen instelling te worden gedeeld, belangrijk is tevens om het extern te communiceren. De buitenwereld moet op een transparante manier kennis kunnen nemen van het morele kompas dat de organisatie hanteert.

Transparantie is tevens van belang om de uitgangspunten voor het gebruik van data analytics en AI goed te borgen. Het ontwerp van dergelijke systemen moet voldoen aan dataprincipes en dient allerlei risico's te adresseren op gebied van ontwerp, algoritme, performance en resilience. Het is aan instellingen zelf om te voorkomen dat maatschappelijke grenzen worden overschreden.

Uitgangspunten borgen

Een lastige vraag blijft natuurlijk: waar liggen die grenzen precies? Waar wet- en regelgeving ontoereikend blijken te zijn, is dat een vraag die elke instelling voor zichzelf zou moeten beantwoorden. Daarbij gaat het veel meer om een ethisch vraagstuk dan om afwegingen rond de bescherming van persoonsgegevens. Dit is eens te meer van belang om de uitgangspunten voor het gebruik van data analytics en AI goed te borgen. Het ontwerp van dergelijke systemen dient te voldoen aan ethische en sociale normen en de uitkomsten die het genereert moeten betrouwbaar zijn. Menselijke *biases* kunnen niet worden getolereerd. Want dat leidt niet alleen tot resultaten die de klant onwelgevallig zijn, maar die ook apert onjuist zijn. Dat zou voor elke instelling een aansporing moeten zijn om beleid in de vorm van duidelijke standaarden te ontwikkelen op het gebied van data ethics. Het simpelweg afzijdig blijven op het gebied van data analytics en AI is overigens geen optie. Met de komst van deze technologieën worden bestaande businessmodellen namelijk in hoog tempo herschreven. Dus wie zich afzijdig houdt, zet zichzelf buitenspel.

Tony de Bos
Partner EY Financial Services Advisory
T +31 (0)6 29 08 41 82
E tony.de.bos@nl.ey.com


30
8
23

Amerikaanse toestanden?

Door Gerrit-Jan Zwenne

Een jaar geleden werd de AVG ingevoerd en dat is niet onopgemerkt gebleven. Al dan niet vanwege de aangekondigde hoge boetes proberen bedrijven en instellingen zo goed en zo kwaad als het kan te voldoen aan de nieuwe privacyregels. Gemakkelijk is dat niet altijd. Aan de formele vereisten, zoals het bijhouden van een verwerkingsregister, is nog wel betrekkelijk eenvoudig te voldoen. Wat er precies in zo'n register moet staan, is een andere vraag. Over de meest eenvoudige AVG-verplichtingen is er al discussie. Daarnaast bevat de AVG ook nog eens een heleboel open begrippen en vage normen. Er zijn gelukkig veel privacy-adviseurs om organisaties bij te staan. En sommigen beloven dat ze uw bedrijf of instelling honderd procent AVG-compliant zullen maken. De vraag is in hoeverre deze adviseurs dergelijke claims kunnen waarmaken. Want wat precies wel en wat precies niet mag is vaak nog maar in beperkte mate duidelijk.

Waarom worden de regels niet opgehelderd? Een verklaring daarvoor is dat er nog niet heel veel gerechtelijke procedures zijn geweest over de privacywetgeving, zodat er nog weinig rechtspraak is over hoe de regels moeten worden uitgelegd en toegepast. En dat houdt weer verband met de omstandigheid dat het vaak heel lastig is om aan te tonen dat een privacy-inbreuk inderdaad heeft geleid tot een bepaalde schade. Als het gaat om een overduidelijk datalek is het maar de vraag of de slachtoffers daarvan erin slagen aan te tonen dat de onterechte creditcardafschrijvingen het gevolg zijn daarvan. Voor een individu is dat een zaak met geringe slagingskansen.

Binnenkort gaat dat misschien veranderen. De AVG en de Wet massaschade maken het gemakkelijker om met claimstichtingen, vergelijkbaar met Loterij-verlies en Woekerpolis, te gaan procederen over privacy-inbreuken. Als een toezichthouder een substantiële boete heeft opgelegd, ligt het voor de hand dat een claimstichting een procedure begint en namens gedupeerden schadevergoeding vordert. Zelfs als het gaat om betrekkelijk geringe bedragen – zeg 250 euro per gedupeerde – kan het al rendabel zijn om met vijf- tot tienduizend gedupeerden een zaak te beginnen. En gelet op de omvang van sommige inbreuken kan zo'n stichting mogelijk nog heel veel meer gedupeerden achter zich krijgen.

Amerikaanse toestanden!? Ik hoor het u denken. Misschien zien we straks inderdaad advertenties van *privacy ambulance chasers*. Maar is dat erg? Ik weet het eerlijk gezegd niet. Ik denk dat ook dergelijke procedures kunnen bijdragen aan een betere privacybescherming. En omdat we ook moeten erkennen dat de middelen van privacy-toezichthouders nu eenmaal beperkt zijn, is er wel wat te zeggen voor dit soort particuliere initiatieven. Maar ik moet erbij zeggen dat mijn beeld, als advocaat die graag procedeert over privacyzaken, misschien wat gekleurd is.

Gerrit-Jan Zwenne is hoogleraar te Leiden en advocaat te Den Haag

Een jaar na dato is de AVG niet langer voer voor juristen alleen

Veel organisaties hielden in het voorjaar van 2018 een race tegen de klok om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Hoe staan zij er een jaar later voor? De conclusie van de round table over dit thema: financiële instellingen praten eigenlijk nauwelijks meer over de AVG maar maken wel meer dan ooit zorgvuldige afwegingen over een verantwoorde omgang met (persoonlijke) data. Een gesprek met Jeffrey Bholasing (Global Head Data Quality & Data Protection bij ING), Duco Tuinenburg (Head General Legal Affairs & Oversight bij NN Group) en Saskia Vermeer-de Jongh (Advocaat en partner bij HVG Law) onder leiding van Rudo Gischler (EY).

Gischler: 25 mei 2018. Bij veel betrokkenen staat deze datum nog in het geheugen gegrift als de harde deadline waarop de AVG van kracht werd. De mensen aan tafel waren er alle drie in verschillende rollen nauw bij betrokken. Hoe kijken zij erop terug?

Tuinenburg: "Het was hard werken, maar het leverde ook een momentum. Om een groot internationaal bedrijf als Nationale-Nederlanden in beweging te krijgen is veel inspanning nodig, maar daar staat tegenover: als die beweging eenmaal op gang is dan is die beweging ook niet meer te stoppen en wil iedereen binnen Nationale-Nederlanden dit goed en zorgvuldig doen. Toen het besef over het belang van het thema in 2016 breed begon te leven, kwam er veel op gang."

> "We gebruiken drie simpele criteria. Kunnen we het? Mogen we het? En willen we het?

Bholasing: "AVG was bij ING onderdeel van een beweging die sowieso al in gang was gezet. Data protection was al geruime tijd een belangrijk punt."

Vermeer: "Klinkt goed. Ik heb destijds ook voorbeelden gezien waar dat heel anders was. Dat we in maart/april nog werden gebeld of we mensen beschikbaar hadden om te helpen hun organisatie AVG-compliant te maken. Organisaties die zich zo kort tevoren pas gingen voorbereiden ontkwamen soms niet aan houtje touwtje oplossingen. Wat overigens een rol speelde bij die last minute benaderingen is dat er ook met de deadline in zicht weinig guidance van de toezichthouders was over wat organisaties precies moesten doen."

> Ethiek van data-gebruik wordt steeds meer een issue

Gischler: Het risico van een harde deadline is dat er daarna 'AVG-moeheid' optreedt. Dat iedereen blij is dat de deadline is gehaald en dat de aandacht wegebt. Hoe ervaren jullie dat?

Vermeer: "Mijn ervaring is dat veel partijen na de implementatiedatum de juiste vragen gingen stellen, juist omdat de druk van de 'deadline' eraf was. Ze gingen nadenken over wat de AVG nu echt betekent voor hun organisatie. Er wordt inmiddels eigenlijk nauwelijks meer gepraat over

Jeffrey Bholasing
Global Head Data Quality & Data Protection bij ING

AVG, maar wel heel veel over data governance. Tegelijkertijd zie ik ook dat er (nog) weinig handhaving is, en dat daardoor een prikkel ontbreekt voor partijen die deze prikkel misschien nog wel nodig hebben."

Bholasing: "Data privacy is bij ING van meet af aan meer dan een juridisch onderwerp en is gaandeweg steeds meer multidisciplinair ingestoken. Er is binnen ING een breed gedragen besef dat data privacy voor onze klanten en werknemers essentieel is, we geen incidenten willen en dat het vooral geen 'legal only' onderwerp is. Die multidisciplinaire aanpak borgen we binnen ING onder andere met een Data Protection Sounding Board, een interdisciplinair overleg op hoofdkantoorniveau waar operationele stappen worden besproken en uitgewerkt."

Tuinenburg: "Die multidisciplinaire aanpak is heel herkenbaar en ook nodig om privacy ook echt *by design* in je systemen te krijgen. Ik denk dat vooral IT en Information Risk een steeds grotere rol zijn gaan spelen in dit dossier. En het mooie is: zij vinden het ook erg leuk om dat te doen."

Gischler: De lastige juridische vragen zijn inmiddels wel beantwoord. Zijn er nog domeinen waar dilemma's spelen?

Tuinenburg: "Die zijn er zeker, alleen zijn ze minder van strikt juridische aard. Als voorbeeld: er is Nationale-Nederlanden veel aan gelegen om nauwgezet met data en persoonsgegevens om te gaan. Omdat onze klanten dat verdienen en omdat we als beursgenoteerd bedrijf zorgvuldig

Saskia Vermeer-de Jongh
Advocaat en partner bij HVG Law

omgaan met onze reputatie. Maar 'zorgvuldig met data en persoonsgegevens omgaan' hoeft niet gelijk te staan aan het 'sec' voldoen aan wet- en regelgeving, het gaat verder dan dat."

Gischler: Handelen binnen de letter van de wet zonder te kijken en na te denken over de ethics rondom data. Daarmee komen we op dit punt niet meer weg?

Tuinenburg: "Zeker niet. Als wij plannen ontwikkelen waar het gebruik van data een rol speelt gebruiken we drie simpele criteria. Kunnen we het? Mogen we het? En willen we het?"

Bholasing: "Die laatste vraag is heel relevant en niet altijd gemakkelijk te beantwoorden. We kiezen bij twijfel voor de veilige weg, in de wetenschap dat we verassingen voor onze klanten willen voorkomen. Er zijn tal van business-

cases te bedenken waar je met de koppeling van externe en interne databronnen proposities kunt maken, die toegevoegde waarde voor onze klanten kunnen hebben. Maar bij al die opties vragen we ons steeds weer af of onze klant dat ook wil en in hoeverre keuzevrijheid geborgd is."

Tuinenburg: "Technologie trekt zich niets aan van wetgeving en ontwikkelt zich in een rap tempo door. Wetgeving hobbelt daar per definitie achteraan. Daardoor ontstaan vraagstukken waar de wet soms geen antwoord op geeft. Je hebt dan eigenlijk een maatschappelijke norm nodig. Maar die is er niet."

Vermeer: "Ethiek van datagebruik wordt steeds meer een issue. Het is inderdaad zoeken naar de norm. Zowel ten aanzien van de maatschappelijke opinie als ten aanzien van de

Duco Tuinenburg
Head General Legal Affairs & Oversight bij NN Group

> "Wetgeving hobbelt per definitie achter de techniek aan

invulling van de wettelijke eisen. Je ziet partijen ook hoopvol kijken naar de toezichthouder op dit vlak, maar die geeft nog weinig handvatten. In zekere zin zou het helpen als er een paar cases voor de rechter komen. Maar geen enkele financiële instelling wil daar natuurlijk de vingers aan branden en dus lijkt iedereen de veilige route te bewandelen."

Tuinenburg: "We willen als financiële instelling onze bijdrage leveren om de norm te bepalen. We kijken daarvoor ook naar de politiek en partijen zoals bijvoorbeeld VNO/NCW of het Verbond van Verzekeraars om daar een rol in te spelen."

Bholasing: "Overigens gaat het bij de dilemma's op dit punt niet altijd om aantasting van privacy, maar ook om andere aspecten. Vanuit de wetenschap is bijvoorbeeld het vraagstuk bekend om met data-analyse de risico's van hypothecaire leningen in te schatten. Dat kan interessante inzichten opleveren."

Gischler: Alles overziend. Kiezen financiële instellingen dan nu niet een wat erg veilige benadering?

Bholasing: "Onze eigen medewerkers zijn een goed kompas om op te varen als het gaat om de ethiek van wat we doen. Want zij zijn vaak ook onze klanten. Wat in het licht van data privacy ook een rol speelt is PSD2. Deze richtlijn maakt het mogelijk dat nieuwe partijen na toestemming van de klant toegang krijgen tot de betaaldata van die klant in de systemen van de bank. Het wordt interessant om te zien hoe partijen hier invulling aan gaan geven en waar klanten een voorkeur voor hebben. Bijvoorbeeld of zij bereid zijn om gegevens te delen in ruil voor een commercieel aanbod."

Tuinenburg: "We willen het gewoon goed doen. Maar het punt is: het valt niet op als je het goed voor elkaar hebt, alleen maar als je steken laat vallen. Neem bijvoorbeeld de mogelijkheid tot het doen van een zogenaamd inzageverzoek, het recht op inzage in je persoonsgegevens, zoals voorgeschreven in de AVG. We hebben dat bij Nationale-Nederlanden echt mooi ingericht en onze klanten kunnen met een druk op de knop al inzicht krijgen in hun persoonsgegevens en contacten met ons. Daar is veel aandacht aan besteed. Maar voor zaken die gewoon goed geregeld zijn is er minder aandacht."

Vermeer: "Ten aanzien van bijvoorbeeld het onderwerp profiling – waarmee je bepaalde voorkeuren van mensen in kaart brengt - leven er veel vragen en zit iedereen een beetje naar elkaar te kijken wat er wel en niet mag. In algemene zin denk ik dat we daar soms overdreven voorzichtig in de wedstrijd zitten. Als je heel feitelijk kijkt naar wat er in de AVG staat mag er meer dan je wellicht denkt."

Zeven vragen AVG-certificering

De beste manier voor bedrijven om de buitenwereld te laten zien dat ze voldoen aan de AVG-privacywetgeving, is door zich te laten certificeren. We vroegen Jatin Sehgal, Managing Partner EY CertifyPoint en expert op het gebied van certificeringsprocessen, om uit te leggen waar het allemaal om draait.

1 Wat is AVG-certificering?

"De burgers van de EU en de EEA (European Economic Area) willen dat gegevensverwerkers verantwoordelijk worden gesteld voor de verwerking van hun gegevens met passende privacymaatregelen. Een keurmerk in de vorm van een onafhankelijke certificering door een betrouwbare en onpartijdige partij helpt daarbij. Op grond van artikel 42 van de AVG-verordening, is de AVG-certificering een goedgekeurd middel om aan te tonen dat zij zich aan de regels houden en vertrouwen in de markt opbouwen."

2 Wat is het doel daarvan?

"Het doel van het certificeringssysteem voor gegevensbescherming in het kader van de AVG is organisaties te helpen aantonen dat zij voldoen aan de eisen van de verordening voor hun activiteiten als verwerker van persoonsgegevens, controleur ervan of allebei. Organisaties die het belang van de privacy van een individu erkennen, transparantie handhaven en de datalevenscyclus adequaat beheren, kunnen niet alleen voor hun klanten, maar ook voor de maatschappij in het algemeen talrijke voordelen opleveren."

3 Kun je een paar voordelen noemen?

"Het eerste voordeel is een concurrentievoordeel en een grotere acceptatie van de producten en diensten van de organisatie. Ten tweede toont de certificering aan dat de organisatie door een derde partij als voldoende volwassen wordt beschouwd om persoonlijke gegevens van EU-ingezetenen te verwerken. Ten derde levert het bewijs van naleving naar belanghebbenden zoals klanten en regelgevers. Tot slot zorgt het voor meer interne transparantie, wat leidt tot vertrouwen binnen de organisatie als ook naar de markt."

4 Wat is de scope van de certificering?

"De opbouw van de AVG en de toepasbaarheid ervan op de verwerking van persoonsgegevens is het belangrijkste aspect. De AVG-regelgeving vereist dat een certificatiemechanisme in het kader van AVG betrekking moet hebben op een gegevensverwerkingsactiviteit. Een dergelijke activiteit kan gedeeltelijk of integraal deel uitmaken van een product, een systeem of een dienst. De certificering moet worden verleend met betrekking tot de verwerkingsactiviteit of -activiteiten. Organisaties moeten dus weten waar ze de grens moeten trekken en welke activiteiten binnen de scope vallen en dus moeten worden gecertificeerd."

5 Hoe ziet het proces van het verkrijgen van een certificering eruit?

"Het proces voorziet in een beoordeling van de opzet van het AVG compliance programma van de organisatie. De beoordeling vindt plaats aan de hand van de wettelijke vereisten waarin o.a. het volgende wordt meegenomen: verwerkingsactiviteiten, producten en diensten, technologieën, locaties, processen, informatiemiddelen, mensen. Tijdens dit proces is een auditor ook geïnteresseerd of de opzet in werkelijk-

heid bestaat en de werking daarvan effectief is. Het certificeringsproces maakt gebruik van algemeen aanvaarde audittechnieken, waaronder het beoordelen van documentatie, interviews en observaties, om te beoordelen of de organisatie aan de gestelde eisen voldoet. Het is een meerjarige cyclus en bestaat uit jaarlijkse korte toezichtaudits om de naleving van de regelgeving te beoordelen."

6 Voor welke uitdagingen staan bedrijven?

"AVG is niet slechts een wettelijke verplichting die je erbij doet. Het heeft verstrekkende gevolgen voor de hele organisatie, met inbegrip van de manier waarop organisaties omgaan met o.a. technologie, klantbenadering en overige verkoopactiviteiten - in feite geldt dat ook voor de hele toeleveringsketen. Organisaties in de EU en in de hele wereld hebben nu al te maken met de druk van regelgevende instanties, maar ook van klanten, leveranciers en partners om zich aan de regels te houden. Zij zitten organisaties op de hielen om aan te tonen dat deze zich houden aan de regels op het gebied van privacybeheer. Dit heeft er inmiddels toe geleid dat bedrijven hun interne privacy- en juridische teams hebben versterkt om de reacties op regelgevers en klanten te beheren, wat tot veel interne inefficiënties heeft geleid. Dit is precies waar AVG-certificeringsmechanismen nuttig zijn, omdat ze bedrijven in staat stellen om een onafhankelijke evaluatie van hun privacy- en gegevensverwerkingsactiviteiten openbaar te maken. Daarnaast kunnen zij ook profiteren van de kennis van een auditor om een duidelijke strategie voor de naleving van het AVG vast te stellen."

7 Wat zien we in de huidige markt?

"Hoewel de verordening al sinds vorig jaar van kracht is, beginnen de gegevensbeschermingsautoriteiten nu pas te praten over het overnemen van AVG-certificeringsregelingen van certificeringsinstanties. Het Europees comité voor gegevensbescherming heeft de certificeringsrichtsnoeren pas onlangs gepubliceerd. We zien dat er een mogelijk risico bestaat dat er een gebrek aan harmonisatie bestaat tussen certificatieschema's uit verschillende gegevensverwerkingsovereenkomsten en dus van wederzijdse erkenning van certificatie-instellingen. Een andere mogelijkheid is dat er Code of Conduct-certificaten zullen worden ingevoerd en dat er nieuwe ontwikkelingen plaatsvinden met betrekking tot een aanstaande ISO-norm voor Privacy Information Management Systems. Daarmee wordt het er niet eenvoudiger door."

Jatin Sehgal
Managing partner EY CertifyPoint
T +31 (0)6 29 08 48 25
E jatin.sehgal@nl.ey.com

EY | Assurance | Tax | Transactions | Advisory

Over EY
EY is wereldwijd toonaangevend op de gebieden assurance, tax, transaction en advisory services. Met de inzichten en de hoogwaardige diensten die wij bieden, dragen wij bij aan het versterken van het vertrouwen in de kapitaalmarkten en economieën overal ter wereld. Wij brengen toonaangevende leiders voort die door samen te werken onze beloften aan al onze stakeholders waarmaken. Daarmee spelen wij een cruciale rol bij het creëren van een beter functionerende wereld voor onze mensen, onze cliënten en de maatschappij.

De aanduiding EY verwijst naar de wereldwijde organisatie en mogelijk naar een of meer lidfirma's van Ernst & Young Global Limited (EYG), die elk een afzonderlijke rechtspersoon zijn. EYG is een UK company limited by guarantee en verleent zelf geen diensten aan cliënten. Voor meer informatie over onze organisatie, kijk op ey.com.

Over EY's Financial Services
Wet- en regelgeving voor financiële ondernemingen wordt steeds strikter. Banken en verzekeraars staan voor de uitdaging om naast het effectief beheersen van risico's ook te voldoen aan verwachtingen van uiteenlopende belanghebbenden. Vermogensbeheerders en dienstverleners zien zich dagelijks gesteld voor uitdagingen als het beheersen van de organisatiegroei, risicovermindering, het bieden van transparantie en het accepteren van toezicht. EY stelt desgewenst een wereldwijd opererend team van deskundigen samen om u te helpen uw mogelijkheden maximaal te benutten. Onze mensen beschikken over zeer uitgebreide ervaring op het gebied van Assurance, Tax, Transaction en Advisory. Bovendien zijn zij uitstekend toegerust om u te helpen inspelen op trends in de markt zodat u uw doelen kunt verwezenlijken en effectiever kunt concurreren. Zo maakt EY het verschil.

© 2019 Ernst & Young Accountants LLP.
Alle rechten voorbehouden.

ED None
155010519

MIX
Papier van verantwoorde herkomst
FSC® C121163
FSC www.fsc.org

Dit document is uitsluitend bedoeld ter algemene informatie en niet als accountancy, fiscaal of anderszins professioneel advies. Gelieve voor specifiek advies contact op te nemen met uw adviseurs.

ey.com/nl

© 2019 EYGM Limited. All Rights Reserved. ED None.