

Interview

Waar het gaat om de bescherming van persoonsgegevens, ligt het sluitstuk van good governance bij de raad van commissarissen, vindt **Aleid Wolfsen**, voorzitter van de Autoriteit Persoonsgegevens. Er komt een leidraad. ‘Dit is een grondrechtendiscussie.’

Door **Philip Willems**



Philip Willems is zakenjournalist en adviseur. Eerder was hij onder meer chef economieredactie bij *Elsevier Weekblad* en hoofdredacteur van *Management Scope*.

'GRONDRECHTEN VAN DE MENS ZIJN OOK HET TERREIN VAN DE RVC'

VIERLUIK

4

Voor een goed gesprek met voorzitter Aleid Wolfsen van de Autoriteit Persoonsgegevens (AP) is, zoals hij het zelf benoemt, 'een aanloopje nodig'. Want zeker, de verwerking van persoonlijke data in Europees verband is een hot topic. Techgigant Google kreeg in Frankrijk onlangs een boete van 50 miljoen, en diens concurrent Amazon zou in Luxemburg aankijken tegen een boete van 350 miljoen euro. Maar hoe zijn we hier ook alweer gekomen?

Europese lidstaten tuigden de afgelopen jaren gestaag wetgeving en bijhorende toezichtorganisaties op, om te voldoen aan de Europese regelgeving rondom persoonlijke databescherming: de GDPR of *General Data Protection Regulation*. De reikwijdte en gevolgen van wat we in Nederland kennen als de Algemene Verordening Gegevensbescherming (AVG), worden pas nu duidelijk. Sinds de introductie van de wetgeving in mei 2018, lag de nadruk in eerste instantie op de effecten voor bedrijven en andere organisaties: wat moeten zij doen om het goed te doen? Voor kleine bedrijven ontstonden vraagstukken

als: hebben we wel een privacyverklaring en is die accuraat? Wat doen we met persoonsgegevens die we via onze website verzamelen, zoals bij het gebruik van zogeheten *tracking cookies*? Hebben we eigenlijk wel toestemming om die gegevens te verzamelen? Hoe zijn de verwerkingsovereenkomsten geregeld?

Voor grote organisaties ontstonden een stuk complexere vraagstukken. Is er sprake van een verplicht verwerkingsregister bijvoorbeeld, en hoe borgen we ons interne toezicht op alle processen rondom gegevensverwerking?

Anno 2021 gaat ook handhaving steeds meer een rol spelen. Het boetebeleid van de AP is er tot op heden vooral op gericht grote organisaties te straffen bij misstanden. In 2021 kreeg het OLVG-ziekenhuis in Amsterdam een boete van 440.000 euro omdat onbevoegde werknemers te makkelijk bij medische dossiers konden komen. Reisorganisatie Booking.com kreeg een boete van 475.00 euro omdat het een datalek

te laat had gemeld. In Europees verband overigens vallen die bedragen dus nog mee.

Een stortvloed aan boetes voor kleinere ondernemingen (bijvoorbeeld omdat ze hun cookie-instructies net niet goed hebben geregeld) is vooralsnog uitgebleven. Al tonen twee recente boetes dat de AP zich vanaf 2021 toch ook echt op de kleintjes richt, of begint te richten. In juni van dit jaar kreeg een orthodontiepraktijk een boete van 12.000 euro wegens dataverwerking op een slecht beveiligde website.

De Autoriteit Persoonsgegevens kortom, richt zich in hoofdzaak op educatie, maar laat ook steeds vaker de tanden zien. Het is tegen deze achtergrond dat het gesprek met Aleid Wolfsen plaats heeft. Directe aanleiding voor het gesprek: Wolfsen heeft aan *Goed Bestuur & Toezicht* laten weten dat de AP werkt aan een data-leidraad voor commissarissen.

De AP werkt aan een leidraad, specifiek over datalekken en specifiek voor de commissaris. Hebben commissarissen het al niet druk genoeg?

‘We hebben net het driejarig bestaan gevierd van de AVG. Die wetgeving komt voort uit het zogenoemde Handvest van de grondrechten van de Europese Unie, dat van kracht is sinds 2009. We kenden in Europa al het grondrecht op privacy. Daarnaast werd in het Handvest een nieuw grondrecht gecreëerd, namelijk op de bescherming van persoonsgegevens. In onze huidige tijd van digitalisering is dat grondrecht enorm belangrijk. Ik kan bijvoorbeeld veel van mijn privacy prijsgeven door van alles en nog wat over mezelf op internet te plaatsen. Dan kan iedereen dat zien. Maar hoe gaan we er mee om als andere mensen die data van het scherm *scrapen* om er bestanden mee op te bouwen? Daarom werden privacy en het recht op bescherming van gegevens twee verschillende grondrechten, die je afzonderlijk prijs kunt geven. Dat prijsgeven gebeurt in twee situaties. Een: als er wetgeving is die de verwerking van jouw data toestaat. Twee: als je zelf toestemming hebt gegeven om jouw data te verwerken. In beide gevallen geldt dat goed is omschreven wat mag en niet mag. Dan de praktijk. Sinds mei 2018 hebben we heel veel tijd

en energie gestopt in het uitleg geven aan wat de AP de verwerkingsverantwoordelijken noemt: bedrijven en hun besturen. Hen spreken we aan als er een lek is of als er te veel data worden verwerkt, of als er wordt gediscrimineerd, bijvoorbeeld via fouten in algoritmes. Dus inderdaad, commissarissen zijn niet het eerste aanspreekpunt. Maar we vinden dat de toezichthouder wel een duidelijke verantwoordelijkheid heeft. De raad van toezicht heeft vier taken: het benoemen van de accountant, toezicht houden, het werkgeverschap van de raad van bestuur, en tot slot gevraagd en ongevraagd adviseren. Bij de tweede en de vierde taak, het adviseren en het toezicht, moet je als commissaris ook risico's inschatten. Die zijn waar het persoonsgegevens aangaat heel reëel. Er is geen bedrijf meer dat geen data verwerkt. Omdat databescherming een grondrecht is, is het beheren van die data een grote maatschappelijke verantwoordelijkheid van bedrijven. Dus commissarissen moeten zich in deze materie verdiepen.’

De leidraad is bedoeld als een stukje educatie?

‘We willen commissarissen activeren en stimuleren om na te gaan wat er in hun bedrijf gebeurt rondom data. Dat is nodig. Neem als extreem voorbeeld de bankencrisis. Toen die in 2008 ontstond, bleek dat commissarissen geen idee hadden wat voor producten banken verkochten. Het ging om hele complexe financiële producten, die dan vaak werden doorverkocht. De bestuurder wist niet hoe de vork in de steel zat en de commissaris wist het al helemaal niet. Inmiddels zijn producten nog complexer worden. En dit type financiële producten, maar ook producten van andere aanbieder, zijn bovendien heel erg, wat wij gedatificeerd noemen. Daar moet je je in verdiepen om het te kunnen begrijpen.’

Hoe slecht gaat het wat betreft datalekken en andere dataproblemen in ondernemingen?

‘Met de bewustwording van het thema gaat het echt de goede kant op. Maar het probleem zelf wordt niet minder. Het aantal meldingen neemt toe. Dat komt

A portrait of Aleid Wolfsen, a middle-aged man with glasses, wearing a dark suit, white shirt, and patterned tie. He has his arms crossed and is standing in front of a blurred background of stone steps.

‘Ik zou het verstandig vinden als de digitale commissaris in de Corporate Governance Code wordt opgenomen’

deels door het toegenomen bewustzijn, waardoor het aantal ontdekte gevallen toeneemt. Maar je ziet natuurlijk ook dat het thema digitalisering accelereert – en daarmee ook de problemen. Overigens is het ook gewoon een goed idee dat tijdig bij ons te melden. Wij kunnen dan snel meekijken en adviseren. Hoe voorkom je verdere schade? Moeten mensen nieuwe wachtwoorden? Is er iets structureel mis in het bedrijf? Moet je mensen of instanties informeren?’

Is de gemiddelde commissaris inmiddels voldoende digi-fähig?

‘Ons beeld is dat dit op veel plekken onder de maat is. Bedrijven stellen vaker een commissaris aan die de digitale wereld snapt. Maar eigenlijk gebeurt het nog te weinig. Het is bij elk bedrijf doodnormaal dat minstens één commissaris verstand heeft van geld, ook als dat bedrijf geen financiële instelling is. Wij denken: alles

Aleid Wolfsen

(1960) begon zijn loopbaan als parketmedewerker bij de arrondissementsrechtbank in Zwolle. Tegelijkertijd studeerde hij rechten aan de Rijksuniversiteit Groningen. Tot 2002 bleef hij werkzaam in de rechtspraak, onder andere als griffier, rechter en bestuurder. In 2002 werd hij Tweede Kamer-lid voor de PvdA, en in 2008 burgemeester van Utrecht. Sindsdien 2016 is hij voorzitter van de Autoriteit Persoonsgegevens. Tevens vervult hij een aantal nevenfuncties, waaronder het voorzitterschap van de raad van commissarissen van drinkwaterbedrijf Oasen en het voorzitterschap van de raad van muziekrechtenorganisatie Sena.

wat met data en de digitale wereld te maken heeft, is zeker zo relevant als de financiën.’

Moet er in dat geval naast de voor veel bedrijven verplichte auditcommissie ook een digicommissie komen?

‘Dat zou een route kunnen zijn. Een andere route is dat digitale expertise standaard aan de auditcommissie wordt toegevoegd.’

Een digicommissie hoeft dan niet, maar een digicommissaris wel?

‘De aanstelling ervan zou ik bij alle bedrijven heel verstandig vinden. Ik zou het ook heel verstandig vinden als in de Nederlandse Corporate Governance Code wordt opgenomen dat in bedrijven waar serieuze hoeveelheden data aanwezig zijn, er ook iemand in de raad van commissarissen zit die de digitale wereld begrijpt. Vroeger waren de grootste concerns ter wereld olie- en gasbedrijven. Nu zijn dat datagedreven ondernemingen. Dat zegt wel wat over al die ondernemingen die daar achteraan komen: daar mikken er heel veel van ook op data, of ze maken er op zijn minst gebruik van. Daarnaast hebben veel bedrijven op grond van de AVG een verplichte Functionaris Gegevensbescherming (FG). Die FG is beschermd door de wet en kan niet worden ontslagen. Hij of zij heeft ook toegang tot het bestuur of tot de commissarissen. De commissarissen moeten erop letten dat die positie goed geborgd is. In de dialoog tussen bestuur en commissarissen wordt digitalisering steeds belangrijker. Ik denk overigens ook dat veel bestuurders ook wel blij zouden zijn als er iemand in de RvC met hen hierover kan praten. Besturen is vaak een eenzaam beroep.’

U noemt de Corporate Governance Code. Heeft u in bredere zin een boodschap voor de Monitoring Commissie Corporate Governance Code?

‘Ga met dit thema aan de slag: in het kader van profielen, van opleiding, van alles eigenlijk wat met scholing te maken heeft.’

U benadrukt hoe belangrijk het thema gegevensbescherming is. Toch zullen commissarissen misschien zeggen: ook al is bescherming van persoonsgegevens een groot thema, het gaat hier over kwaliteit van uitvoering. Dan wordt het al snel een operationele kwestie...

‘Sinds de AVG in werking is getreden, zie je dat accountants in hun jaarverslag paragrafen over de omgang met datalekken en digitale gegevens zijn gaan opnemen. Een bedrijf dat data heeft moet, zoals dat heet, voldoende organisatorische en technische maatregelen nemen om lekken te voorkomen en de beveiliging op orde te hebben. Als het fout gaat, kun je grote boetes krijgen. Overigens zeg ik niet dat iemand met digitale expertise zich alleen met data bezig moet houden. Denk bijvoorbeeld aan grote ICT-projecten. Die mogen dan een uitvoeringskwestie zijn, een bedrijf kan er behoorlijk mee de bietenbrug opgaan.’

Vandaar ook uw suggestie om digitale expertise in de auditcommissie onder te brengen.

‘Ja. Maar wat ik als commissaris nóg belangrijker zou vinden dan de financiële en accounting-aspecten, is het vertrouwensaspect. Want als jouw databestanden weglekken, of als er ontstaat discriminatie door een algoritme, raakt dat de kern van het bedrijf. Reputatieschade bij de klanten ligt al snel op de loer.’

Een laatste vraag over die digicommissaris: is dat een jonge commissaris?

‘Bij jongeren is de digitale kennis vanzelfsprekender, maar ik zou het toch ook voor een belangrijk deel in scholing zoeken. Want zoals ik in het begin van dit gesprek aanstipte, voor een belangrijk deel gaat dit gesprek niet over bits en bytes, maar over grondrechten. Het verwerken van data en gegevens heeft te maken met vrijheid, autonomie en het zelfbeschikingsrecht van mensen. Daar moeten commissarissen in thuis zijn.’

Vrijheid en zelfbeschikkingsrecht: u noemt daar nogal een thema. Met de opmars van de techgiganten, maar zeker ook met de opmars van afwijkende wereldbeelden in de internationale politieke arena, is zelfbeschikkingsrecht een groot thema aan het worden.

‘Inderdaad: in de westerse wereld zijn we opgegroeid met deze vrijheden. Door de digitalisering en de snelheid waarmee deze oprukt, komen die hier en daar echt in de verdrukking. De Nederlandsche Bank en de Autoriteit Financiële Markten hebben een jaar geleden organisaties waar zij toezicht houden – in hoofdzaak banken en verzekeringsmaatschappijen – nog gewaarschuwd: pas op bij het gebruik van algoritmes met het voorspellen van het gedrag van mensen. De bias die je zelf hebt, wordt vaak meegeprogrammeerd. Voor je het weet, ben je discriminerend bezig, bijvoorbeeld omdat je mensen gaat uitsluiten van je diensten.’

Hoever kun je bedrijven vragen te gaan in rechtschapen gedrag? Kom je dan niet ook op het domein van politieke keuzes?

‘Dat vind ik niet. Bij de vorige presidentsverkiezingen in de Verenigde Staten en ook met de Brexit, zag je dat bedrijven via micro-targeting en algoritmes op een oneigenlijke manier bijstand gaven aan de verkiezingen. Die waren feitelijk bezig met het manipuleren van de verkiezingen. Dan ondermijnt je de democratie. Neem ook weer de uitdaging van de algoritmes. Als jij sollicitanten uitnodigt, en daar een algoritme voor gebruikt dat uitsluit op leeftijd, seksuele voorkeur of etnische achtergrond.’

Bedrijven moeten zich gewoon aan de wet houden en daar hebben commissarissen een rol in te spelen?

‘Ja. De wet legt de waarden vast die we met z’n allen belangrijk vinden: gelijkwaardigheid, en grondrechten als vrijheid van geloof en niet discrimineren. Dat nieuwe grondrecht overigens, bescherming van je gegevens, is een soort moeder van al die andere

grondrechten aan het worden. Dat is een leuke gedachtenoefening: alle grondrechten hebben op de een of andere manier met de bescherming van persoonsgegevens te maken.’

Laten we de praktijk bekijken: wat komt er in uw leidraad?

‘Ten eerste: agendeer het thema in de RvC. Kijk of de deskundigheid er is en of die goed genoeg is. Kijk wat de corebusiness van je bedrijf is. Als je tot de conclusie komt dat naast je product en financiën er veel sprake is van digitalisering, dan moet je iemand in de raad van commissarissen hebben die dat begrijpt. Zorg voor je eigen opleiding, zodat je de risico’s kunt inschatten van het gebruik van algoritmes. Zodat je niet zonder dat je het eigenlijk doorhebt alleen nog blanke mannen van middelbare leeftijd aan het aannemen bent, om maar wat te zeggen. Dat je begrijpt wat accountants zeggen als ze commissarissen aanspreken met de vraag: hebben jullie het hier een beetje op orde qua lekken en beveiligen?’

Sommige besturen en commissarissen zullen zeggen: pfff, een leidraad. Waar moeten we ons nu weer aan houden? Is het niet voldoende dat de wet er is en de dreiging van boetes?

‘Die houding moet kantelen. We maken een leidraad om commissarissen te helpen intrinsiek gemotiveerd te raken. Je moet het willen, niet moeten. Die boetes zijn het worst case scenario. Voor commissarissen moet het eigenlijk ook een beetje leuk zijn om hiermee bezig te zijn. Commissarissen moeten in ieder geval een keer per jaar met de controller praten. Zo moet je ook een keer per jaar met de Functionaris Gegevensbescherming praten. Als er geen FG is, moet je met de chief information officer praten, en sowieso met je directie. Niet om zelf te gaan besturen, maar om je te laten informeren over hoe het ervoor staat in het bedrijf.’