

Een jaar na start handhaving:

# NOG LANGE WEG TE GAAN OM VOLLEDIG AVG COMPLIANT TE WORDEN

Nu we bijna een jaar onderweg zijn met de Algemene Verordening Gegevensbescherming rijst de logische vraag: hoever zijn we nu eigenlijk? Regine Scholten van Brieq Advocatuur in Leiden is gespecialiseerd in dit onderwerp en zij is nog niet meteen laaiend enthousiast. 'Er is veel gebeurd, maar er moet misschien nog wel veel meer gebeuren.'



“

*‘Maar je mag feitelijk niet eens bellen met de vraag hoe het echt met je zieke medewerker gaat.’*



‘Tot vorig jaar 25 mei, D-day voor wat betreft de inwerkingtreding van de handhaving van de nieuwe privacywetgeving, werkte je je als advocaat in dit vakgebied een slag in de rondte. Er waren veel partijen behoorlijk nerveus voor die bewuste datum. Nu die dag voorbij is, lijkt de storm te gaan liggen. Een beetje als bij de Millenniumbug destijds. Maar is dat in dit geval terecht? De realiteit is namelijk een stuk weerbarstiger. Het gaat bij privacybescherming en informatiebeheer niet om één moment. Het gaat juist om beheersbaarheid en continuïteit voor de langere termijn.’

#### VEEL WAS ER AL

De paniek rondom ‘D-day’ vorig jaar was volgens haar overigens zwaar overtrokken. ‘Veel van wat in de AVG staat, was ook al van kracht onder de Wet bescherming persoonsgegevens. Natuurlijk, er zijn zaken aangescherpt en de boetes bij overtredingen met name zijn veel hoger. Maar de rechtsgronden waren er al; de doelbinding voor het verzamelen van gegevens was er ook al. Die hogere boetes zijn feitelijk één van de belangrijkste verschillen. En dat overall in Europa (binnen de EU althans) nu dezelfde basis geldt.’

De problematiek rondom efficiënt en effectief informatiebeheer, die voldoet aan alle richtlijnen in de wet is echter nog precies hetzelfde, ziet Regine. ‘Hoe bepaal je wat je mag bewaren, hoe lang mag/moet je het bewaren en hoe categoriseer je informatie zodanig dat je snel en duidelijk inzicht hebt in wat er eigenlijk binnen jouw systemen aanwezig is? Er gelden uiteenlopende wettelijke bewaartermijnen voor verschillende informatietypen. Dat zijn veelal minimum termijnen. Financiële gegevens moet je tenminste zeven jaar bewaren. Met de nieuwe wet worden persoonsgegevens gekoppeld aan een maximum bewaartermijn, die erop neer komt dat je persoonsgegevens niet langer

mag bewaren dan voor het doel waarvoor ze zijn verzameld noodzakelijk is. De essentie van de nieuwe privacywet is dat je daar als organisatie actief op anticipeert. Een sollicitatiebrief met cv bijvoorbeeld mag je niet langer bewaren dan vier weken als de sollicitant afgewezen wordt, tenzij de kandidaat

## COOKIETRACKERS ZONDER TOESTEMMING

Dat nog niet iedereen zich met veel enthousiasme aan de regels houdt, bleek onlangs toen bekend werd dat ruim dertienhonderd Nederlandse websites zogenaamde cookietrackers plaatst op de apparaten van de bezoekers. Ook als de bezoeker daar geen toestemming voor geeft. Dat bleek uit een onderzoek van de NOS. Die cookies werden gebruikt om zo advertenties op maat te kunnen aanbieden bij volgende zoekacties. De Autoriteit Persoonsgegevens gaat nu zelf onderzoek doen. Het is nog steeds een discussie of het stilzwijgend instemmen met het plaatsen van cookies is toegestaan. Daarover buigt de rechter zich nog.



toestemming geeft om die gegevens 'in portefeuille te houden'. Met toestemming geldt in principe een termijn van één jaar. Zou je dat toch nog langer willen dan moet je wel goede redenen hebben en periodiek die kandidaat actief benaderen of het nog steeds is toegestaan. Je kunt niet na één vraag die gegevens maar tot het 'einde der tijden' in je gegevensverzameling houden. Het categoriseren van de informatie is dus van essentieel belang: welke informatiecategorie wordt gekoppeld aan welke bewaartermijn en wanneer moet het worden verwijderd/vernietigd? Dat is een voortdurend en dynamisch proces, want er gaat steeds weer nieuwe informatie rond in een organisatie. Die dynamiek maakt het lastig te beheersen als je daar niet consequent aandacht aan besteedt.'

### PAKKANS MINIMAAL

Nu is het niet zo dat wanneer je niet aan de AVG voldoet je het risico loopt dat je volgende week iemand van de Autoriteit Persoonsgegevens op de stoep hebt staan. De pakkans met andere woorden, is niet zo groot, eigenlijk minimaal. Regine: 'Misschien. Het gaat er echter ook om dat privacy ingebakken raakt in het arbeidsethos van de medewerkers en de organisatie als geheel. Je moet het willen doen. Niet alleen omdat de wet het voorschrijft, maar omdat je beseft dat het professioneel, belangrijk en beter is voor alle betrokkenen. Iedereen moet ervan doordrongen zijn dat het heel vervelend is wanneer gevoelige of persoonlijke gegevens op straat komen te liggen of worden misbruikt. Niemand vindt het prettig dat bedrijven je lastig vallen of met jouw gegevens geld proberen te verdienen, terwijl jij daar geen toestemming voor hebt gegeven. Dat is dan wel wat meer vanuit de AVG geregeld: je hebt als 'eigenaar' van je eigen persoonsgegevens



*'Met de nieuwe wet worden persoonsgegevens gekoppeld aan een maximum bewaartermijn. De essentie van de nieuwe privacywet is dat je daar als organisatie actief op anticipeert.'*



*'Maar hoe staat het met de veiligheid van die gegevens die je op die mobiele devices gebruikt? Ik heb nog niet de indruk dat daarin nu zoveel is veranderd.'*

wat meer daadwerkelijk het recht om daar wat aan te doen. Het bewustzijn bij die eigenaren van de gegevens is een stuk groter geworden. Zij wijzen organisaties snel op hun 'fouten'. Die fouten vinden echt niet altijd direct met opzet plaats. Integendeel, vaak zullen ze meer voorkomen door ingesleten werkmethodes.'

### WETTEN EN REGELS SCHUREN LANGS ELKAAR

Dat fouten voorkomen, is volgens haar ook niet zo verwonderlijk als je bedenkt dat een aantal regels en wetten langs elkaar 'schuren'. Regine: 'Neem de AVG en de Wet Poortwachter, die werkgevers verplicht om van alles te doen aan re-integratie van hun zieke werknemer. Maar je mag feitelijk niet eens bellen met die zieke werknemer om inhoudelijke vragen over zijn ziekte te stellen, terwijl een belangstellende leidinggevende vaak juist wel zou willen weten wat zijn medewerker mankeert om hem of haar zo goed mogelijk te kunnen helpen en weer op de been te helpen. Ook wil een werkgever natuurlijk graag weten of er wellicht andere manieren zijn om de zieke werknemer weer snel in het arbeidsproces in te schakelen, bijvoorbeeld door aangepast werk of aangepaste omstandigheden die het toch mogelijk maken (deels) weer aan de slag te gaan.'

Burgers als consumenten zijn wijzer geworden. In het geval van het gebruik van paspoort of ID-bewijzen zijn individuele burgers als consumenten inmiddels wel een stuk wijzer geworden. 'Ook bedrijven weten inmiddels dat ze niet zomaar om het paspoort mogen vragen om er een kopietje van te maken. Dat gebeurde voorheen aan de lopende band bij hotels en dergelijke. Nu weten mensen vaak dat er niet om een kopie mag worden gevraagd. Er zijn zelfs apps die een digitale kopie leveren, waarbij de belangrijkste en gevoeligste gegevens zijn 'geblurd'. Daaraan merk je dat de wereld wel aan het veranderen is en zich bewuster

wordt van de risico's wanneer je al te makkelijk met je persoonlijke gegevens omgaat. Zo ook met maatschappelijke ontwikkelingen als Uber: de 'taxichauffeur' weet aan de hand van de app precies waar je bent, maar jij weet ook alles van de locatie van die taxi en wie erin zit om je op te halen. Waar blijven die gegevens? Is dat allemaal geborgd? Het zou wel moeten in ieder geval.'

## GROTE GEVAREN IN MOBIELE TOEPASSINGEN

Volgens Regine zit een groot gevaar dan ook in al die apps en mobiele toepassingen waarvan we zo graag gebruik maken. 'Toepassingen als WhatsApp, Facebook en dergelijke die je net zo makkelijk ook op je smartphone gebruikt. Wie maakt geen gebruik van Google Maps als navigatie? Al die apps leggen veel gegevens vast.

REGINE SCHOLTEN: 'JE MOET WEL ZORGEN DAT MENSEN DE REGELS ZELF OOK LOGISCH VINDEN, ANDERS GAAN ZE EROMHEEN EN GEBEURT ER NIETS.'





*'Een pragmatische aanpak is geboden: zorg ervoor dat het allemaal werkbaar, behapbaar en duidelijk blijft. Daarin blinkt deze wet niet helemaal uit helaas...'*

Dat weten we inmiddels wel en dat het niet altijd goed geregeld is, weten we inmiddels ook, maar er zijn nog zoveel meer toepassingen. We maken ook al volop gebruik van bedrijfsgegevens op een tablet of smartphone en vinden het de normaalste zaak van de wereld dat we alle gegevens onderweg op de telefoon kunnen raadplegen. Maar hoe staat het met de veiligheid van die gegevens die je op die mobiele apparaten gebruikt? Ik heb nog niet de indruk dat dit altijd even goed is geregeld.'

### **BEGIN BIJ HET BEGIN**

Maar het begint bij het begin, de informatie op orde. Regine: 'Daar hoort – naast weten wat je hebt - ook bij dat je moet weten wie welke gegevens gebruikt. Zowel intern als extern. Zijn daarvoor de verwerkersovereenkomsten al geregeld? Wat staat daar precies in? Is de informatie daarmee geborgd als er iets mis dreigt te gaan of al is gegaan? Dat laatste geeft op dit moment veel extra werk. Veel bedrijven overzien het niet meer en vragen ons dan om die verwerkersovereenkomsten op te stellen en af te handelen. De eerste vraag die je je echter moet stellen, is of het eigenlijk wel nodig is dat je zo'n verwerkersovereenkomst afsluit. Niet iedere organisatie of ieder bedrijf aan wie je gegevens verstrekt, is meteen een verwerker. Arbodiensten hebben bijvoorbeeld een afwijkende positie. Zij moeten immers gebruik kunnen maken van specifieke gegevens om mensen (terug) te begeleiden naar werk. Het zijn echt complexe vraagstukken: wie is de verwerker en wie is de verwerkingsverantwoordelijke en in welke gevallen moet je een verwerkersovereenkomst sluiten? Dat bepalen, is echter dermate specialistisch werk dat organisaties daar zelf vaak weinig heil in zien. Wat je veel ziet, is dat de risico's al snel bij een

ander worden neergelegd. Zelfs dat leveringsvoorwaarden verkapt in de verwerkersovereenkomst worden ingebakken. Als dan de samenwerkingspartner niet tekent, heeft hij de opdracht niet. Maar het is helemaal niet terecht dat organisaties dergelijke voorwaarden inbouwen.'

### **PRAGMATISCHE AANPAK GEBODEN**

Het is kortom nog geen gelopen koers, die AVG. 'Sterker nog', aldus Regine, 'er is nog heel veel niet helemaal – of zelfs helemaal niet – geregeld in de markt. Ook na een jaar van inwerkingtreding van de handhaving is het nog altijd geen gemeengoed dat informatie en informatiestromen op orde zijn en dat organisaties precies weten wat waar is en wie daarvan om welke reden gebruik maakt. Dat is echter wel de essentie van de wetgeving. Binnen bepaalde markten, zoals de HR of de juridische markt, is al wel heel veel op orde. Logisch misschien, omdat ze daar wellicht meer de juiste competenties in huis hebben, maar ook voor andere markten geldt die urgentie. De AVG is vooral een grote stap gebleken in de richting van meer aandacht voor compliancy en privacy. Je moet voldoen aan de wet, maar laat het vooral zoveel mogelijk aansluiten bij de bestaande werkwijze van de medewerkers. Praktisch en herkenbaar geven meer resultaat. Teveel pushen

zou averechts kunnen werken. Dan zoeken ze alternatieven en ben je veel verder van huis. Geef dat bewustzijn de tijd om te rijpen. Er komen tegelijkertijd ook kansen voor nieuwe oplossingen voor bijvoorbeeld beveiligde platforms met gereguleerde toegang tot gegevens. Daarmee los je wellicht veel problemen een stuk sneller op, mits de processen rondom informatie transparant, veilig en betrouwbaar plaatsvinden.'

