ANJA DEKHUIJZEN
COLUMN
CIO MAGAZINE
JULI 2019

GDPR BOETES in EUROPA: HOGE BOETES IN ENGELAND EN REVOLUTIONAIR BOETEBELEID IN NEDERLAND

Een jaar na de invoering van de GDPR wordt door velen de eerste balans opgemaakt. De kruitdampen zijn opgetrokken, de meeste paniek is voorbij. Wat heeft de nieuwe privacywet Europa gebracht? Is het schrikbeeld van torenhoge boetes bewaarheid?

Wanneer men met name de Engelse boetes van de afgelopen tijd volgt, zou men de indruk kunnen krijgen van wel. Zo maakte de Engelse toezichthouder, de ICO, recent haar voornemen bekend om een boete van omgerekend € 205 miljoen op te leggen aan British Airways inzake een datalek. Zoals bekend kan men onder de GDPR niet een boete opgelegd krijgen voor een datalek zelf. Wel kan men een boete van € 10 miljoen of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar (de hoogste van de twee) opgelegd krijgen als het datalek is veroorzaakt doordat de achterliggende beveiligingsmaatregelen van het bedrijf niet toereikend waren, of als men ten onrechte het datalek te laat of helemaal niet meldt. Met name voor multinationals kan dit flink in de papieren lopen.
In het onderhavige geval waren volgens de ICO de gebrekkige beveiligingsmaatregelen er de oorzaak van dat 500.000 klanten van British Airways werden omgeleid naar een andere, frauduleuze website, waar vervolgens hun persoonsgegevens werden gestolen.
Op 8 juli 2019 schreef Elizabeth Denham van de ICO in een sweeping statement: "*People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights*.".

Dat de ICO goed op stoom is gekomen blijkt uit een tweede bericht van de afgelopen tijd, namelijk een voorgenomen boete van omgerekend bijna € 110 miljoen aan Marriott. Ook hier betreft het diefstal van persoonsgegevens, in dit geval van ongeveer 339 miljoen klanten, als gevolg van een datalek door gebrekkige beveiliging. Het zal voor sommigen een verlossing lijken dat de ICO als gevolg van de Brexit mogelijk minder te zeggen krijgt bij cross-border datalekken in de EU.

In Nederland vaart de Autoriteit Persoonsgegevens (de AP) een andere koers. Vooralsnog geen torenhoge boetes. Wel een gedetailleerd beleid, vrijwel als enige in de EU, gepubliceerd in de Staatscourant, over hoe de AP eventuele boetes in de toekomst zal berekenen ter bevordering van "*rechtsgelijkheid en rechtszekerheid*". De AP blijkt een revolutionaire koers te varen. Want met name ten aanzien van niet-ondernemingen neemt de AP in vrijwel alle gevallen afstand van de boetes onder de GDPR, welke kunnen oplopen tot 2 of 4% van de totale wereldwijde jaaromzet. Voor deze groep worden boetes van maximaal een ton tot ongeveer een miljoen in het vooruitzicht gesteld. Daarnaast blijkt uit de boetebeleidsregels dat de AP in de praktijk voor ondernemingen tot ongeveer 50 werknemers in veel gevallen bereid is om eveneens de lagere boetes als maximum te hanteren. Daar staat wel iets tegenover, wat weinig van doen lijkt te hebben met rechtsgelijkheid. Voor grotere ondernemingen en multinationals stelt de AP dat deze de hoge GDPR boetes kunnen krijgen opgelegd, als de aangepaste lagere boetes geen passende bestraffing zijn, "*waarbij kan worden gedacht aan het gewicht van de overtreder uitgedrukt in de jaaromzet*". Oftewel, het feit dat men in financieel opzicht een grote onderneming is, lijkt reden om een hoge boete op te leggen. Dit staat haaks op het boeteregime van de GDPR. De GDPR noemt 11 redenen om de hoogte van een boete vast te leggen, zoals de aard en de ernst van de overtreding. De financiële omvang van de overtreder wordt niet genoemd. Het zal interessant zijn om te zien of de AP daadwerkelijk financiële draagkracht van grote ondernemingen gaat meewegen bij het bepalen van boetes, en of de rechter dit zal sanctioneren.