FORUM

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

BART VAN DER SLOOT - 13.02.2018

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming van de Europese Unie van toepassing. De Verordening bevat maar liefst 88 pagina's aan gedetailleerde regels, met niet minder dan 99 wetsartikelen en 173 overwegingen die uitleg geven aan die artikelen. In de AVG staan regels over bewaartermijnen, restricties voor het verzamelen en delen van gegevens, voorwaarden voor het verwerken van gevoelige gegevens, bijvoorbeeld over iemands gezondheid of ras, en regels over het melden van datalekken. Ook staan er verplichtingen in over transparantie, impact assessments, documentatie, organisatie inrichting en de beveiliging van gegevens.

Het belangrijkste is misschien dat er sanctiemogelijkheden in de Verordening zijn opgenomen. Als een persoon of organisatie niet voldoet aan de regels uit de Verordening dan kan per overtreding een boete worden opgelegd van een bedrag oplopend tot € 20,- miljoen of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dat meer is dan € 20,- miljoen. Daarbij staan in de Verordening ook andere mogelijke gevolgen beschreven, zoals aansprakelijkheid voor een overtreding of het wereldkundig maken van een overtreding, wat reputatieschade kan betekenen voor bedrijven.

De Algemene Verordening Gegevensbescherming bouwt voort op de EU Richtlijn bescherming persoonsgegevens uit 1995, die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens. Omdat er in de Richtlijn weinig mogelijkheden waren opgenomen om boetes of sancties op te leggen, hebben veel organisaties nog niet alle regels uit die Richtlijn en de daarop gebaseerde wet geïmplementeerd. In mei 2018 moet er dus in feite een dubbelslag worden geslagen. De regels uit de Richtlijn moeten helemaal worden geïmplementeerd binnen alle procesonderdelen van de organisatie én de nieuwe bepalingen uit de Verordening moeten worden meegenomen.

Waarom wordt de Richtlijn uit 1995 eigenlijk vervangen door een Verordening? De meest gehoorde reden is dat de oude regels uit de tijd voor de internet- en technologieëxplosie komen en dat de regels dus aan vervanging of op zijn minst herziening toe zijn. Dat klopt niet. De meeste regels uit de Richtlijn blijven gewoon van kracht en er zijn geen echte versoepelingen doorgevoerd om meer

technologische innovatie of commerciële exploitatie van persoonsgegevens mogelijk te maken, ondanks een sterke lobby vanuit het bedrijfsleven. De vijf belangrijkste redenen om de Verordening aan te nemen zijn:

1. *Harmonisering regels*
Er bestonden grote verschillen in de manier waarop landen van de Europese Unie de regels uit de Richtlijn in hun nationale wetgeving hadden geïmplementeerd. Daardoor werd de doorvoer van persoonsgegevens tussen die landen, bijvoorbeeld Nederland en Duitsland, bemoeilijkt. Een organisatie moest zich in Duitsland toch weer aan andere regels houden dan in Nederland. Bovendien zorgde dit ook voor een zwakke positie van het datasubject, omdat bedrijven zich vaak vestigden in landen met een soepele interpretatie van het gegevensbeschermingsrecht. Het is belangrijk om te benadrukken dat het gegevensbeschermingsrecht niet alleen tot doel heeft burgers te beschermen tegen bedrijven en overheidsdiensten die hun persoonsgegevens verwerken, maar ook om het vrije verkeer in gegevens binnen de EU, en waar mogelijk naar andere landen, mogelijk te maken. Veel bedrijven en organisaties zijn immers afhankelijk van het verwerken van persoonsgegevens voor hun bedrijfsvoering. De EU wil burgers beschermen, maar tegelijkertijd ook digitale innovatie door middel van persoonsgegevens mogelijk maken. Het probleem dat verschillende landen de regels uit de Richtlijn anders hadden geïmplementeerd in hun nationale wetten wordt nu aangepakt door het aannemen van een Verordening in plaats van een Richtlijn.

2. *Harmonisering handhaving*
Het tweede probleem was dat de handhaving van de gegevensbeschermingsregels nog steeds op landelijk niveau gebeurde. Hierdoor was er ook verschil in hoe actief de regels werden gecontroleerd en afgedwongen in verschillende EU-landen. Dit had onder meer tot gevolg dat internationale bedrijven zich vestigden in landen waar de regeldruk laag en de handhaving van de regels beperkt was. Ierland is daar naar verluid een voorbeeld van. Dit probleem wordt aangepakt doordat de Verordening meer inzet op handhaving van de regels door de EU zelf en er meer samenwerkingsmogelijkheden zijn voor de verschillende nationale handhavingsinstanties. In Nederland heet de handhavingsorganisatie de Autoriteit Persoonsgegevens.

3. *Versterking handhaving*
Omdat er weinig mogelijkheden waren voor sancties en boetes waren neergelegd in de Richtlijn bescherming persoonsgegevens, was de praktijk dat niet alle bedrijven en organisaties het even nauw namen met de gegevensbeschermingsregels. Deze regels kregen vaak simpelweg geen prioriteit op board-room niveau. Om hier verandering in te brengen worden er in de Verordening mogelijkheden geboden om zeer hoge sancties en boetes op te leggen. Ook hebben de handhavingsorganisaties veel extra middelen en bevoegdheden gekregen om strenger en effectiever op te treden.

4. *Democratisering handhaving*
Het gegevensbeschermingsrecht ging primair uit van controle en handhaving vanuit de door de overheid ingestelde handhavingsorganisatie. Dat idee van een toezichthouder stamde uit begin jaren '90, toen dataverwerking nog veel minder prominent was. Omdat nu eigenlijk alle bedrijven en overheidsorganisaties persoonsgegevens verwerken en gegevensverwerking niet een aparte sector is die kan worden gereguleerd (zoals bijvoorbeeld de financiële sector of de medische sector), maar de standaard is in vrijwel alle sectoren, is het bijna ondoenlijk om van overheidswege alle datastromen goed te controleren. Vanwege de beperkte middelen van de handhavende organisaties werd in de praktijk een deel van de markt vrijgelaten. Ook hier brengt de Verordening verandering in. Enerzijds krijgen handhavingsorganisaties meer bevoegdheden en middelen, anderzijds wordt een deel van de regeldruk verlegd naar de gegevensverwerkende organisaties zelf. Een voorbeeld daarvan is dat veel organisaties een impact assessment moeten doen alvorens met een gegevensverwerkingsinitiatief te beginnen, accountable zijn voor alle verwerkingen van persoonsgegevens die door of namens hen worden gedaan en een Data Protection Officer moeten aanstellen, die er binnen de organisatie zelf op toeziet dat alle regels worden nageleefd. De toezicht op en handhaving van de regels wordt dus primair neergelegd bij organisaties zelf; pas als dat fout gaat zal de Autoriteit Persoonsgegevens hoeven op te treden.

5. *Bewustwording*
In de Richtlijn stond een klein aantal rechten van datasubjecten, de personen over wie persoonsgegevens worden verwerkt. Een van de problemen van het gegevensbeschermingsrecht is dat veel burgers niet weten welke rechten ze hebben en het ze soms ook weinig kan schelen wat er met hun gegevens gebeurt. De Verordening tracht hier verandering in te brengen door meer informatie aan individuen te geven over wat er met hun gegevens gebeurt en door hen meer controle te geven over het gegevensverwerkingsproces.

Naast de plichten voor dataverwerkende organisaties, zoals dat zij nauwgezet moeten documenteren welke gegevens zij verwerken, voor welk doel, hoe lang en met wie de gegevens worden gedeeld, krijgen individuen over wie gegevens worden verzameld ook tal van rechten. Zo is er het recht om vergeten te worden, het recht op inzage en het recht op dataportabiliteit, wat zo veel wil zeggen als dat burgers in bepaalde gevallen aan een organisatie mogen vragen om de gegevens die over hen beschikbaar zijn aan een andere, concurrerende organisatie over te dragen. Bij veel organisaties moet nog het nodige gebeuren om, zoals dat heet, *GDPR-compliant* te zijn [GDPR is de Engelse afkorting voor General Data Protection Regulation]. De Autoriteit Persoonsgegevens heeft in ieder geval gevraagd om een sterke uitbreiding in bemensing. Het is afwachten welke organisatie de twijfelachtige eer ten deel zal vallen om de eerste administratieve boete opgelegd te krijgen.

Dit is een voorpublicatie van het boek: De Algemene Verordening Gegevensbescherming in gewone mensentaal, dat te verkrijgen is via de Amsterdam University Press.