GDPR, AVG, FG, DPO, AP, PIA...snapt u het nog?

De aangekondigde implementatie van de General Data Protection Regulation binnen de Europese Unie, oftwel de GDPR, zorgt momenteel voor een stroom aan afkortingen. In deze public briefing nemen we u graag mee wat de afkortingen allemaal betekenen en wat hun functie is als de nieuwe privacy wetgeving binnen de EU lidstaten in mei 2018 geïmplementeerd moet zijn.

Door: Maurice van der Woude[1]

Eerst maar eens beginnen met een verklarende woordenlijst. Met alle afkortingen wordt het sowieso lastig om deze public briefing verder te lezen:

AVG	Algemene Verordening Gegevensbescherming
GDPR	General Data Protection Regulation, in het Nederlands "AVG"
CBP	College Bescherming Persoonsgegevens
AP	Autoriteit Persoonsgegevens, voorheen CBP
FG	Functionaris Gegevensbescherming
DPO	Data Protection Officer, in het Nederlands "FG"
PIA	Privacy Impact Assessment

Algemeen

De Europese privacyverordening algemene verordening gegevensbescherming (AVG) gaat over de 'bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'. Deze verordening vervangt de databeschermingsrichtlijn uit 1995. Die sloot niet meer aan op de huidige digitale wereld en men wilde een regulering invoeren die voor ALLE europese lidstaten zou gelden, in tegenstelling tot de huidige versnipperde wetgeving binnen de landen van de Europese Unie in het kader van (de verwerking van) privacygevoelige

[1]Maurice van der Woude is vice-voorzitter van Stichting Cloud Community Europe Nederland en CEO bij BPdelivery B.V.

gegevens.

Waar gaat het globaal over
De AVG/GDPR gaat over (bescherming van) persoonsgegevens die met name in databanken worden opgeslagen en waarvan ontsluiting rechtstreeks kan leiden naar een natuurlijk persoon. De algemene principes die hierbij gehanteerd moeten worden zijn de volgende:

- transparantie: de persoon van wie de gegevens verwerkt worden, is hier van op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.
- doelbeperking: de persoonsgegevens worden voor een welbepaald en wettig doel verzameld, mogen niet voor andere zaken gebruikt worden en niet worden doorgegeven aan andere, niet ter zake doende verzameling(en)
- gegevensbeperking: enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld
- juistheid: de persoonsgegevens moeten correct zijn en blijven
- bewaarbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel
- integriteit en vertrouwelijkheid: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging
- verantwoording: de verantwoordelijke verzamelaar moet kunnen aantonen aan bovenstaande regels te voldoen

Nu al actief
In tegenstelling tot wat veel organisaties denken is de AVG in mei 2016 al in werking getreden. Van organisaties wordt nu verwacht dat zij hun bedrijfsvoering met de AVG in overeenstemming brengen. Zij krijgen daarvoor tot 25 mei 2018 de tijd. Op 6 mei 2018 moeten alle EU-lidstaten deze verordening in hun nationale wetgeving hebben omgezet.

Boetes
25 mei 2018 mag iedereen organisaties op de naleving van de AVG aanspreken. De maximale boete is 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet in het geval van een onderneming, afhankelijk van welk bedrag hoger is.
Opsporingsinstanties en het OM zijn echter van de AVG vrijgesteld, omdat zij onder aparte privacywetgeving vallen.

EU-VS privacy schild
Het EU-VS-privacyschild is een reeds bestaande overeenkomst over de

bescherming van persoonsgegevens van EU-burgers die in de VS worden verwerkt. Deze blijft onder de huidige voorwaarden nog steeds actief, al gaan de discussies daarover nog steeds door.

Autoriteit Persoonsgegevens
De instantie in Nederland die belast is met de uitvoering en instandhouding van deze verordening (en later in 2018 dus wet) is de Autoriteit Persoonsgegevens (AP), voorheen het College Bescherming Persoonsgegevens (CBP). Men kent momenteel de AP van de invoering van de wet datalekken op 1 januari 2016 en dat de AP belast was met de uitvoering van die wet en de naleving ervan binnen Nederland. De AP krijgt er in 2018 nog meer bevoegdheden bij in het kader van uitvoering van de GDPR. De AP kan echter onmogelijk alle Nederlandse bedrijven die persoonsgegevens beheren, controleren. Hiervoor zijn bedrijven die aan bepaalde verwerkingsvoorwaarden voldoen, verplicht een functionaris gegevensbescherming aan te stellen. Deze FG moet dan ook formeel aangemeld worden bij de AP.

Functionaris Gegevensbescherming
Een van de gevolgen van de AVG is dat binnen bedrijven die persoonsgegevens verwerken een Data Protection Officer (DPO), in gewoon Nederlands een Functionaris Gegevensbescherming (FG), aan moeten stellen. De aanstelling van een FG is verplicht onder de volgende organisaties of omstandigheden:

<u>Het betreft een overheidsinstantie of publieke organisatie</u>
Hieronder vallen onder andere rijksoverheid, gemeenten en provincies, maar ook bijvoorbeeld zorg- en onderwijsinstellingen.

<u>Het betreffen organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen</u>.
Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables.

<u>Het betreffen organisaties die op grote schaal bijzondere persoonsgegevens verwerken waar dit een kernactiviteit is.</u>
Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden. Rechtbanken zijn overigens uitgesloten van deze verplichting.

Alhoewel er geen specifieke vereisten in opleiding aan de FG worden gesteld, dient deze conform de richtlijn te voldoen aan minstens de volgende aspecten:

- Hij of zij moet ter zake gedegen kennis hebben van de persoons

gegevens die door de organisatie verwerkt worden
- Hij of zij moet eenvoudig bereikbaar zijn en kunnen communiceren met zowel de (lokale) verwerkers en de nationale toezichthouder
- Hij of zij moet deskundig zijn in het toepassen van de wettelijke bepalingen die in het kader van de AVG gelden
- Hij of zij beschikt over professionaliteit en de benodigde ethiek in het kader van de AVG en de dataverwerkingen
- Er is geen belangenconflict, de FG kan boven de partijen staan maar hoeft niet perse een medewerker van de organisatie zelf te zijn

Privacy Impact Assessment (PIA)
Bedrijven kunnen verplicht zijn een PIA uit te voeren op basis van de gegevens die zij in geautomatiseerde systemen verwerken. Een PIA is een instrument om *vooraf* de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De Rijksoverheid is nu al verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een PIA. Andere organisaties zijn nu nog niet verplicht een PIA uit te voeren. Organisaties die (op termijn) een PIA verplicht uit moeten voeren, zijn die organisaties die ook de verplichting hebben om een FG aan te stellen. Mocht er toch nog twijfel zijn, dan wordt als vuistregel gehanteerd dat als minstens 2 van de 10 onderstaande criteria van toepassing zijn, de organisatie verplicht een PIA dient uit te voeren:

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Doorgifte van persoonsgegevens buiten de EU
10. Blokkering van een recht, dienst of contract

Meerdere landen
Stel dat u een onderneming leidt die in meerdere landen actief is. Dan heeft u met deze nieuwe verordening nog maar met 1 toezichthouder te maken. Dit wordt de 'leidende toezichthouder' genoemd (lead supervisory authority). De leidende toezichthouder is als eerste verantwoordelijk voor het toezicht op organisaties met grensoverschrijdende gegevensverwerkingen. De hoofdregel is dat de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie is gevestigd, de leidende toezichthouder is. Deze coordineert al haar activiteiten in samenwerking met de toezichthouders in de andere landen

waar de organisatie actief is.

Geraadpleegd:
Http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL
Http://privacytrends.nl/overig/vooruitblik-de-gdpr-in-hoofdlijnen/
Http://www.justitia.nl/privacy/data-protection-officer.html
https://nl.wikipedia.org/wiki/Algemene_verordening_gegevensbescherming
https://autoriteitpersoonsgegevens.nl/nl

Wilt u meer informatie naar aanleiding van deze Public Briefing?

p/a Escrow4all
MediArena 7, 1114 BC
Amsterdam-Duivendrecht
Tel: +31(0) 8787 65656
mail: info@cloudcommunityeurope.nl
web: www.cloudcommunityeurope.nl

Over Cloud community Europe
Cloud Community Nederland is de Stichting in Nederland die onafhankelijk de belangen van Cloud Computing aanbieders en afnemers behartigt in het kader van de digitale transformatie. Cloud Community Nederland is verbonden aan de federatie van Nationale Cloud communities met vertegenwoordiging in 8 landen in Europa en 400+ aangesloten Europese bedrijven.