DE ALGEMENE VERORDENING GEGEVENSBESCHERMING : EEN KORT OVERZICHT(*)

De eerste IBM Personal Computer werd 35 jaar geleden, op 12 augustus 1981, geïntroduceerd. De eerste generatie iPhone werd in de Verenigde Staten geïntroduceerd op 29 juni 2007. In het daaropvolgende decennium is de bescheiden mobiele telefoon uitgegroeid tot een multimedia-toestel om te surfen op het web, e-mails te beheren en foto's te maken en te delen. Facebook ging van start in 2004 en Twitter in 2006. Sedert het midden van de jaren '80 is de persoonlijke communicatie via elektronische weg exponentieel gegroeid.

Online platformen en internetbrowsers kunnen "gratis" worden gebruikt, zij het in ruil voor de persoonlijke gegevens van de gebruikers. Er is een duidelijk spanningsveld tussen het recht van het individu op respect voor zijn privé- en familieleven, zijn woning en correspondentie enerzijds, en de ambitie van bedrijven om nieuwe klanten te bereiken op een meer doelgerichte en efficiënte manier, anderzijds.

De technologie is geëvolueerd en de reglementering heeft geprobeerd gelijke tred te houden. Het Verdrag van de Raad van Europa voor de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens werd aangenomen in Straatsburg op 28 januari 1981. Een eerst Richtlijn 95/46/EC betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens werd geïmplementeerd vanaf oktober 1998.

Richtlijn 95/46/EC zal worden ingetrokken en vervangen door de Algemene Verordening Gegevensbescherming (afgekort: "AVG"), in het Engels: "General Data Protection Regulation" (afgekort: "GDPR"), die afdwingbaar is vanaf 25 mei 2018. Het is de ambitie van de AVG om de EU-wetgeving op gegevensbescherming te actualiseren en geschikt te maken voor de 21ste eeuw. Het is een complex stukje wetgeving. De preambule van de AGV telt niet minder dan 173 overwegingen, terwijl de verordening zelf 99 artikelen bevat, verdeeld over 10 hoofdstukken. Hieronder geven we een kort overzicht van de voornaamste bepalingen. (De verwijzingen hebben betrekking op de artikelen van de verordening, tenzij anders vermeld).

Definities, Artikel 4

- **"Persoonsgegevens"** worden in artikel 4 (1) gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"), die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- De "verwerkingsverantwoordelijke" is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 (7)).
- De "verwerker" is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 (8).

(*) Dit document vormt een onderdeel van FLINNs 'GDPR Self-help toolkit' (© 2018 FLINN.law). Noch de toolkit als geheel, noch dit document als onderdeel daarvan houden rekening met de specifieke kenmerken en noden van uw onderneming. Bijgevolg kan het niet als juridisch advies worden beschouwd.

Toepassingsgebied, Artikelen 2 & 3

- **Materieel toepassingsgebied**: De AVG is van toepassing op de gehele of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2.2. voorziet een aantal uitzonderingen hierop).
- **Territoriaal toepassingsgebied**: De AVG heeft een ruim territoriaal toepassingsgebied. Ze is van toepassing op elke verwerking van persoonsgegevens in het kader van de activiteit van een verwerkingsverantwoordelijke of een verwerker die in de EU is gevestigd, ongeacht of de verwerking al dan niet in de EU plaatsvindt. De verordening is ook van toepassing op alle bedrijven wereldwijd die persoonlijke data verwerken van EU-onderdanen om hen goederen of diensten aan te bieden in de EU of om hun gedrag binnen de EU te monitoren.

Beginselen inzake verwerking van persoonsgegevens

- **Artikel 5** geeft de algemene beginselen aan betreffende de verwerking van persoonsgegevens. De verwerking moet "*rechtmatig, behoorlijk en transparant*" gebeuren, en voor een specifiek doel (*"doelbinding")*, waarbij de verwerking toereikend en ter zake dienend moet zijn en beperkt tot wat noodzakelijk is voor dat doel ("*minimale gegevensverwerking*").
- **Het belangrijke nieuwe beginsel van de "*verantwoordingsplicht*"** wordt ingevoerd in artikel 5.2. De verwerkingsverantwoordelijke zal verantwoordelijk zijn voor de naleving van deze algemene beginselen inzake verwerking van persoonsgegevens en zal deze naleving moeten kunnen aantonen.

Rechtmatigheid van de verwerking

- **Rechtmatigheid van de verwerking**: Artikel 6 geeft zes gronden voor een rechtmatige verwerking, zoals noodzakelijkheid voor: (i) de uitvoering van een overeenkomst, (ii) het voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke, (c) de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.
- **Toestemming**: dit is o.i. de belangrijkste rechtmatigheidsgrond voor verwerking. De betrokkene moet zijn toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig geven door een verklaring of door een duidelijke positieve handeling. Hij moet die toestemming te allen tijde kunnen intrekken op even eenvoudige wijze als het geven ervan (artikel 7).

Rechten van de betrokkene, Artikelen 12-23

- Zoals gezegd is transparantie een basisbeginsel in de verwerking van persoonsgegevens.
- De betrokkenen hebben recht op informatie en communicatie over de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal (artikelen 12, 13 en 14).
- De vereiste van transparantie wordt onderbouwd met een aantal specifieke rechten die aan de betrokkenen een eerlijke verwerking van hun persoonsgegevens verzekert. Artikel 15 voorziet in een recht op inzage voor de betrokkenen. Artikel 16 geeft de betrokkenen een recht op rectificatie en wissing van gegevens ("recht op vergetelheid" - '*right to be forgotten*'): Organisaties moeten er over waken dat zij de nodige procedures en technologie voorzien om gegevens te wissen na verzoek daartoe vanwege de betrokkene (artikel 17). Ook is er voorzien in een recht op beperking van de verwerking (artikel 18) en in een recht op overdraagbaarheid van de gegevens (artikel 20).

- Artikel 22 bevat een duidelijk verbod op profilering. De betrokkene heeft het recht niet te worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden en dat enkel is gebaseerd op geautomatiseerde verwerking, waaronder profilering.

De verwerkingsverantwoordelijke en de verwerker, Artikelen 24-32

- **Verantwoordelijkheid van de verwerkingsverantwoordelijke, Artikel 24.** De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen nemen om te waarborgen en te kunnen aantonen dat de verwerking van de persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd.
- **N.B.** *Artikel 30 voorziet dat elke verwerkingsverantwoordelijke een register bijhoudt van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden.* Deze verplichting kan buiten toepassing gelaten worden voor kleine en middelgrote ondernemingen die minder dan 250 personen in dienst hebben ; de Belgische toezichthoudende autoriteit (de Gegevensbeschermingsautoriteit) beschouwt het houden van een dergelijk register echter als een goede praktijk voor alle bedrijven.
- **Verantwoordelijkheid van de verwerker**: de AVG breidt de verantwoordelijkheid uit tot verwerkers die de vereisten uit de verordening niet naleven. **De beveiliging van de verwerking** door passende technische en organisatorische maatregelen, met inbegrip van, naar gelang het geval, pseudonimisering en versleuteling van de persoonsgegevens, is een verplichting die rust op zowel de verwerkingsverantwoordelijke als de verwerker, en dit rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook de risico's die de verwerking teweegbrengt voor de betrokkenen.

Middelen tot naleving

- De AVG omvat een aantal middelen tot naleving. Artikel 25 handelt over de **gegevensbescherming door ontwerp en door standaardinstellingen.** Algemeen gesteld is het de bedoeling van deze bepaling om aan te geven dat het respecteren van de beginselen van dataverwerking en van de vereisten van de AVG moet ingebouwd worden vanaf het ontwerp van toepassingen en verwerkingen, in plaats van pas na te denken over de bescherming van persoonsgegevens na het ontwikkelen of invoeren van dergelijke nieuwe toepassingen of verwerkingen.
- **Artikelen 33 & 34, Melding van een inbreuk in verband met persoonsgegevens.** De vereisten inzake de melding van een inbreuk in verband met persoonsgegevens strekken ertoe om tot een geharmoniseerde praktijk te komen binnen de EU.
- **Gegevensbeschermingseffectbeoordeling** ("Data Protection Impact Assessment", afgekort "DPIA")**, Artikel 35**. Indien een bepaalde verwerking een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (bijvoorbeeld in geval van invoering van een nieuwe technologie), zullen organisaties voor de verwerking een beoordeling moeten uitvoeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens en eventueel voorafgaand aan de verwerking de toezichthoudende autoriteit moeten raadplegen.

Functionaris voor gegevensbescherming ("Data Protection Officer" of 'DPO'), Artikel 37

- **Aanstelling van een DPO** is verplicht in bepaalde gevallen, onder meer wanneer de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in geval van gerechten bij de uitoefening van hun rechterlijke taken.

Een concern kan beslissen slechts één DPO aan te stellen voor al zijn vestigingen, op voorwaarde dat deze vanuit elke vestiging gemakkelijk te contacteren is.

- Volgens een studie van de International Association of Privacy Professionals, betekent dit dat in gans Europa 28 000 DPO's zullen moeten worden aangesteld.
- De DPO kan een natuurlijk persoon of een rechtspersoon zijn. Indien het gaat om een rechtspersoon, dan is het belangrijk dat elk lid van die organisatie dat de functie van DPO uitoefent de artikelen 37 tot 39 respecteert.

Gedragscodes en certificering, Artikelen 40-43

- Instrumenten om de toepassing van de verordening toe te lichten.
- De naleving van gedragscodes (artikelen 40-41) en certificering (artikelen 42-43) worden door de AVG gezien als een aanvaardbaar middel om de naleving van de AVG aan te tonen. Op het ogenblik van het schrijven van deze tekst zijn deze gedragscodes en certificeringen nog in een ontwikkelingsfase.

Doorgiften van persoonsgegevens aan derde landen of internationale organisaties, Artikelen 44-50

- Artikel 44 geeft als algemeen beginsel aan dat doorgiften buiten de EU enkel mogelijk zijn indien aan de voorwaarden uit dit hoofdstuk is voldaan.
- Artikel 45.3 voorziet dat de Commissie kan beslissen dat een derde land een passend beschermingsniveau waarborgt, zodat doorgiften naar dat land mogelijk zijn zonder verdere specifieke toestemming.
- Indien er voor een derde land geen dergelijk adequaatheidsbesluit bestaat, dan mag een verwerkingsverantwoordelijke of een verwerker enkel persoonlijke data doorgeven naar dat derde land indien zij passende waarborgen bieden. Deze passende waarborgen kunnen geboden worden door verschillende instrumenten, waaronder bindende bedrijfsvoorschriften (artikel 47) of het gebruik van standaardbepalingen.

Toezichthoudende autoriteiten, Artikelen 51-59

- Elke lidstaat moet één of meer onafhankelijke overheidsinstanties aanstellen die verantwoordelijk zijn voor het toezicht op de naleving van de AVG. Hun bevoegdheden, taken en competentie worden omschreven in de artikelen 55 tot en met 58.
- **Leidende toezichthoudende autoriteit**: Voor grensoverschrijdende verwerking van persoonsgegevens binnen de EU is er een leidende toezichthoudende autoriteit. In beginsel zal dit de toezichthoudende autoriteit van de hoofdvestiging (zijnde de plaats van de centrale administratie) of van de enige vestiging van een entiteit zijn. Hierop zijn echter uitzonderingen voorzien, en elke toezichthoudende autoriteit zal alleszins competent zijn om een klacht te behandelen die alleen verband houdt met de lidstaat waarvoor ze verantwoordelijk is.

Samenwerking en coherentie, Artikelen 60-67, en het Europees Comité voor Gegevensbescherming, Artikelen 68-76

- Om bij te dragen tot een consequente toepassing van de AVG moeten de toezichthoudende autoriteiten samenwerken, zowel onderling als met de Commissie, in het kader van een coherentiemechanisme.

- Het Europees Comité voor Gegevensbescherming is een onafhankelijk orgaan met rechtspersoonlijkheid. Het bestaat uit de voorzitter van één toezichthoudende autoriteit per lidstaat en de Europese toezichthouder voor gegevensbescherming. Het Comité heeft onder andere als taak geschillen te beslechten en kan bindende beslissingen aannemen in bepaalde gevallen.

Beroep, aansprakelijkheid en sancties, Artikelen 77-84

- **De mogelijke risico's van de niet-naleving van de AVG zijn aanzienlijk.** Sommige inbreuken op de AVG kunnen het voorwerp uitmaken van administratieve geldboeten tot 20.000.000 euro of tot 4 % van de totale wereldwijde jaaromzet van de betrokken onderneming indien dit cijfer hoger is (artikel 83.6). Dit is de maximumboete die is voorzien voor de meest ernstige inbreuken (bijvoorbeeld voor inbreuken op de rechten van de betrokkenen). De maximale boete voor inbreuken van procedurele aard, die als minder ernstig worden beschouwd, is beperkt tot 10.000.000 euro of 2 % van de totale wereldwijde jaaromzet indien dit cijfer hoger is.
- **Middelen die ter beschikking staan van de benadeelde betrokkenen**: het recht een klacht in te dienen bij de toezichthoudende autoriteit, het recht om een doeltreffende voorziening in rechte in te stellen tegen een toezichthoudende autoriteit, en het recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of verwerker.
- **Recht op schadevergoeding**. Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de AVG, heeft het recht om van de verwerkingsverantwoordelijke of van de verwerker schadevergoeding te ontvangen voor de geleden schade.

Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking, Artikelen 85-91

- **Artikel 88 heeft betrekking of de verwerking in het kader van de arbeidsverhouding.** Het laat ruimte voor de lidstaten om nadere regels vast te stellen voor werknemers, hetzij bij wet, hetzij bij collectieve overeenkomst.

Artikelen 92-99 betreffen de implementatie van de AVG

Artikel 99, 2. Bepaalt dat de AVG van toepassing is vanaf 25 mei 2018.