

## De Algemene Verordening Gegevensbescherming: een nieuwe wind, geen orkaan

Jolien Dewaele, 25 januari 2018

*De Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR) heeft de laatste maanden heel wat stof doen opwaaien. De nieuwe Europese regelgeving bevestigt een aantal bestaande principes, maar schuift daarnaast ook nieuwe accenten naar voor. Voor organisaties die de Privacywetgeving in het verleden al hebben toegepast en nageleefd, betekent dit dus een voortzetting van het huidige beleid, aangevuld met een aantal nieuwigheden. In deze bijdrage ligt de focus op de GDPR met als doel om duidelijkheid te scheppen in die specifieke nieuwigheden. De toepassing van die nieuwe accenten vergt echter een basiskennis van de bestaande principes die we als uitgangspunt gebruiken.*

### De algemene principes van databescherming

Zoals in de inleiding aangegeven, bevestigt de GDPR een aantal basisprincipes op het vlak van gegevensbescherming. Logischerwijs vormen deze principes dan ook het uitgangspunt voor iedereen die aan de slag gaat met gegevens binnen zijn organisatie.

#### *Beginselen inzake gegevenskwaliteit*

Wat betreft de gegevenskwaliteit stelt de regelgever dat persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze verwerkt moeten worden.

**Rechtmatig** betekent dat er telkens een grondslag moet zijn voor de verwerking van persoonsgegevens. Dit is vergelijkbaar met bijvoorbeeld de raadpleging van het Rijksregister. Het raadplegen van het Rijksregister mag alleen op basis van gedefinieerde grondslagen.

Een **behoorlijke** verwerking houdt in dat er gehandeld wordt als een 'goede huisvader'.

Om tegemoet te komen aan een **transparante** verwerking, is het van belang dat natuurlijke personen zich moeten kunnen informeren over de verwerking. Naast die informatie geldt ook een communicatie die opnieuw duidelijk moet zijn ten aanzien van die persoon.

#### *Rechtmatige verwerking*

*"Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding")." (art.1b, GDPR).*

Om aan rechtmatige gegevensverwerking te kunnen doen, moeten organisaties ten minste aan één van onderstaande voorwaarden voldoen (art.6 GDPR).

1. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen.
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.

5. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
6. De verwerking is noodzakelijk voor de behartiging van gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De grondslagen voor rechtmatige gegevensverwerkingen zijn niet nieuw. In het kader van de GDPR is het wel van belang om voor elk van die gegevensverwerkingen inzicht te verwerven in deze grondslag. Afhankelijk van de grondslag voor de gegevensverwerking kunnen onder de GDPR verschillende rechten van de betrokkenen voortvloeien. Bijvoorbeeld wanneer de verwerking op toestemming berust heeft de betrokkene het recht om zijn toestemming op eender welk moment in te trekken.

### *Bijzondere categorieën gegevens*

De GDPR definieert verschillende categorieën van gegevens. Het uitgangspunt betreft uiteraard de persoonsgegevens. Daarnaast zijn er ook nog definities opgenomen van genetische gegevens, biometrische gegevens en gegevens over gezondheid. Gezien de gevoeligheid van de diverse categorieën kan verschillen, is het als organisatie ook van belang om inzicht te verwerven in de aard van de gegevens zoals hiervoor beschreven. Die aard van de gegevens kan immers een impact hebben op de maatregelen die een organisatie moet nemen om de verwerking op een veilige manier te laten gebeuren.

### *Rechten van de betrokkene*

De Belgische Privacywetgeving voorziet al in een aantal rechten van de betrokkenen, die ook terugkeren in de GDPR. Die rechten zijn:

- Recht op informatie
- Recht op toegang: verkrijgen van inzage in persoonsgegevens
- Recht op verbetering
- Recht van bezwaar / beperking
- Recht op gegevenswissing (vergetelheid)
- Recht niet te worden onderworpen aan profilering (geen geautomatiseerde besluitvorming op basis van gevoelige gegevens tenzij o.a. toestemming)
- Recht op overdraagbaarheid van gegevens
- Recht op klacht en beroep van betrokkene
- Recht op vergoeding en aansprakelijkheid bij schade

Het recht op overdraagbaarheid is een nieuw recht dat is toegevoegd in de GDPR. Door de uitoefening van dit recht heeft de betrokkene recht om de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische te krijgen.

### *Beveiliging*

Organisaties moeten passende technische en organisatorische maatregelen nemen om het beveiligingsniveau te waarborgen dat is afgestemd op de risico's van de organisatie.

### *Internationale doorgifte*

*“Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts doorgegeven worden indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.” (art.44 GDPR)*

In dit beginsel staat het waarborgen van het passende beschermingsniveau centraal. Organisaties moeten daarom voldoende technische en organisatorische maatregelen nemen.

### Nieuwe accenten in de GDPR

In de bovenstaande paragrafen toonden we aan dat de basisprincipes vanuit de bestaande Privacywetgeving behouden bleven onder de GDPR. Naast die bevestiging van de principes, legt de GDPR ook een aantal nieuwe accenten. We gaan hieronder dieper in op die nieuwe accenten.

De GDPR legt de klemtoon op een **risicogebaseerde benadering** enerzijds en de **verantwoordingsplicht** anderzijds.

Voor de risicogebaseerde benadering vertrekken we vanuit de onderstaande definitie van een risico.

|                        |
|------------------------|
| Risico = kans x impact |
|------------------------|

Een risico is de kans dat dat een incident / bedreiging / ... zich voordoet vermenigvuldigd met de impact die dit heeft op de organisatie. Op basis van de inschatting van de risico's kunnen technische en / of organisatorische maatregelen genomen worden.

De verantwoordingsplicht houdt in dat de verantwoordelijke voor de verwerking in functie van het risiconiveau verantwoordelijk is voor de naleving van de beginselen (conformiteit van de gegevensverwerkingen) én kan aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals: rechtmatigheid, transparantie, doelbinding, juistheid.

### Nieuwe terminologie<sup>1</sup>

#### *Register van de verwerkingsactiviteiten*

Zowel de verantwoordelijke als de verwerker moet verplicht een schriftelijk (of elektronisch) register bij te houden, waarin alle activiteiten worden omschreven waarbij persoonsgegevens worden verwerkt. Dat register bevat onder andere het volgende:

- contactgegevens
- de doeleinden van de gegevensverwerking
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens
- de categorieën van ontvangers van de gegevens
- indien mogelijk de beoogde bewaartermijnen
- indien mogelijk een beschrijving van de beveiligingsmaatregelen

---

<sup>1</sup> Gebaseerd op presentatie Frank Robben

(Bron: <https://www.frankrobben.be/wp-content/uploads/2016/08/20160610nl.pptx>)

### *Data Protection Officer (DPO) / functionaris voor de gegevensbescherming*

De functionaris gegevensbescherming is een persoon die toeziet op de omgang met persoonsgegevens binnen een organisatie en controleert of de organisatie voldoet aan de wet en toepasselijke regelgeving. Hij moet onafhankelijk kunnen functioneren als contactpersoon en mag zowel intern als extern aangesteld worden.

### *Gegevensbeschermingseffectbeoordeling*

Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Één beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

Dergelijke beoordeling is in ieder geval verplicht bij profilering, de grootschalige verwerking van bijzondere persoonsgegevens of monitoring van openbare ruimten. Hierbij wordt vastgelegd waarom, op welke manier en hoelang er persoonsgegevens verwerkt worden. Daarbij moeten de aanwezige risico's in kaart gebracht en beoordeeld worden. In sommige gevallen is het zelfs verplicht om de beoordeling met betrokkenen te bespreken.

### *Privacy by design*

Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen die aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen die zijn opgesteld met als doel de beginselen van gegevensbescherming, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen

### *Privacy by default*

De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de periode waarin zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen er met name voor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Ter illustratie hierbij een aantal voorbeelden van maatregelen die in het kader van privacy by design / default kunnen genomen worden:

- het minimaliseren van de verwerking van persoonsgegevens
- het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, transparantie met betrekking tot de functies en de verwerking van persoonsgegevens
- het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking

- het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren