Grant Thornton

An instinct for growth™

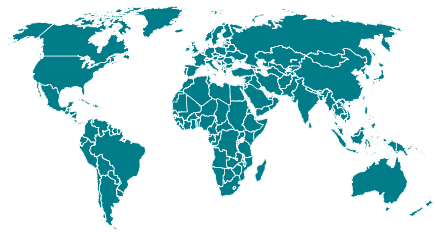
# GDPR (General Data Protection Regulation )

## The journey we take together

# Inleiding

Het Europees Parlement heeft recent de 'General Data Protection Regulation' (GDPR) ofwel de 'Algemene Verordening Gegevensbescherming' (AVG) goedgekeurd. De verordening zal de bestaande **privacyregelgeving harmoniseren** en de huidige Privacyrichtlijn 95/46/EG, die sinds 1995 van kracht is, vervangen. Gezien de GDPR – anders dan de Privacyrichtlijn – rechtstreeks van toepassing wordt in **alle EU-lidstaten**, geldt er voortaan nog maar één wet bescherming persoonsgegevens in de hele Europese Unie.

De GDPR zal vanaf **25 mei 2018** van toepassing zijn. In de aanloop naar deze datum zal het voor organisaties en toezichthouders nodig zijn om zich goed voor te bereiden. De GDPR brengt namelijk heel wat belangrijke nieuwe verplichtingen met zich mee, zodat het voor ondernemingen aangeraden is om nu al actie te ondernemen. De sancties op het niet-respecteren zijn immers aanzienlijk: de toezichthoudende autoriteiten kunnen geldboetes opleggen tot 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet van een onderneming.



# Toepassingsgebied

Het geografisch toepassingsgebied is verruimd: de verordening is niet enkel van toepassing op in Europa gevestigde ondernemingen. Ook buiten de EU gevestigde ondernemingen die goederen of diensten aanbieden op de Europese markt en/of die het gedrag van Europese burgers observeren ('profiling'), zullen aan de nieuwe regels moeten voldoen.

# Wat zijn persoonsgegevens?

**Persoonlijke informatie**

Naam, geslacht, geboortedatum, adres, …

**Online gegevens**

Zoekgeschiedenis, cookies, e-mail, …

**Financiële gegevens**

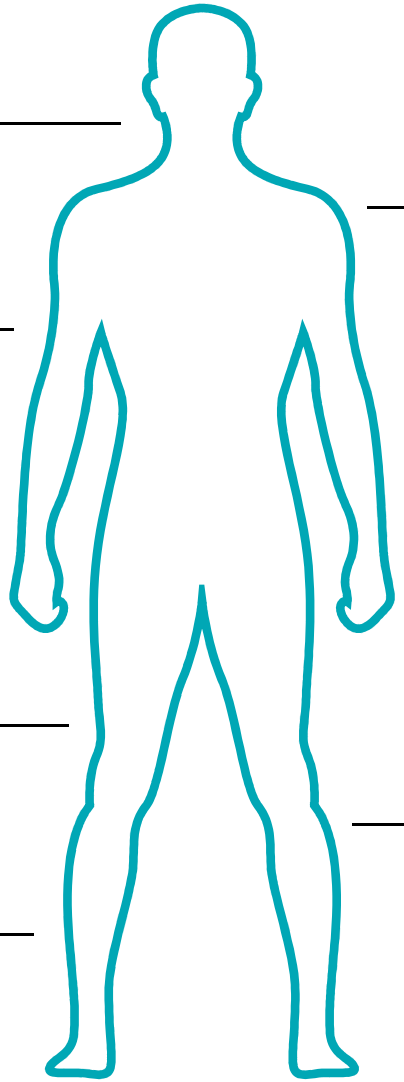
Bankrekening, inkomen, belastingen, …

**Juridische informatie**

Veroordelingen, boetes, …

**Sociale media**

Facebook, LinkedIn, Twitter, …



**GPS gegevens**

Reisinformatie, navigatiesysteem, …

**Medische gegevens**

Vaccinaties, ziekenhuisgegevens,…

**Ethnische gegevens**

Culturele / seksuele voorkeuren, religie, …

**Winkelgedrag**

Winkelaankopen, directe marketing, …

# Definities

De GDPR is van toepassing op verwerkingen van persoonsgegevens. Een verwerking kan worden gedefinieerd als "een (geheel van) bewerking(en) m.b.t. persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, etc. van gegevens". Persoonsgegevens zijn "alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon". Een limitatieve lijst van gegevens die wel of niet kwalificeren als persoonsgegevens bestaat niet, gezien deze kwalificatie steeds afhankelijk is van de situatie.

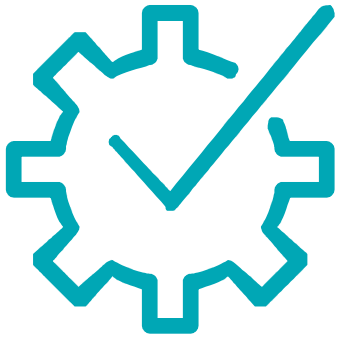
De belangrijkste actoren in de GDPR zijn de betrokkene, de verwerkingsverantwoordelijke en de verwerker. De betrokkene is de (natuurlijk) persoon wiens persoonsgegevens worden verwerkt. Deze krijgt in de GDPR heel wat meer rechten toebedeeld. De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die het doel en de middelen bepaalt van de verwerking.
De verwerker is de natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt.

# Data Protection Officer

Een andere nieuwigheid is dat ondernemingen in bepaalde gevallen een functionaris voor gegevensbescherming of data protection officer (DPO) zullen moeten aanstellen. De DPO is een onafhankelijk adviseur die erop dient toe te zien dat het beleid van de onderneming in overeenstemming is met de verordening. De DPO kan zowel een werknemer als een externe partij zijn. Men doet er als onderneming alvast goed aan om na te gaan of men (in de nabije toekomst) een DPO moet aanstellen.

# Data Protection by Design & by Default

Eén van de grootste nieuwigheden in de GDPR is de introductie van een verplichting tot **gegevens-bescherming door ontwerp** (‘data protection by design') en **als standaardinstelling** ('by default').



Data protection by design houdt in dat men, reeds bij het ontwerpen van nieuwe verwerkingen, de bescherming van persoonsgegevens in acht moet nemen.

De verplichting tot  data protection by default impliceert dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat, per specifiek verwerkingsdoel, in beginsel alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor dat doel. Bijvoorbeeld: indien het voor een bepaald verwerkingsdoel irrelevant is de leeftijd of de geboorteplaats van een persoon te weten, dan zal men er zich van dienen te onthouden deze gegevens bij de betrokkene op te vragen.

# Toestemming

De verwerkingsverantwoordelijke moet de **toelaatbaarheidsgronden** bepalen waarop de verwerking van de persoonsgegevens rusten: **toestemming, contractueel, wettelijke verplichting, vitaal of algemeen belang en gerechtvaardigd belang**. Indien toestemming de grondslag is, dan moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

Expliciete toestemming moet door middel van een **duidelijke, actieve handeling** worden gegeven. Het gebruik van een reeds aangekruist vakje volstaat dus niet. Indien de verwerking meerdere doeleinden heeft, moet voor elk daarvan toestemming worden verleend. De betrokkene heeft tevens het recht zijn toestemming te allen tijde in te trekken.

# Rechten voor betrokkene

Ook voor de betrokkene komen er een heel aantal nieuwe rechten met betrekking tot zijn of haar persoonsgegevens bij.

Zo krijgt de betrokkene in de eerste plaats het **recht van inzage** in de persoonsgegevens die verwerkt worden en in de verwerkingsdoeleinden, de betrokken categorieën van persoonsgegevens, enz. Daarnaast krijgt de betrokkene het recht om onjuiste persoonsgegevens te laten verbeteren en om onvolledige persoonsgegevens te laten vervolledigen. Ook heeft de betrokkene het recht om zijn persoonsgegevens te laten verwijderen, het zogenaamde **recht om vergeten te worden**. Dit recht stelt de betrokkene in staat om persoonsgegevens te laten verwijderen wanneer er geen legitieme reden meer is om deze te bewaren.

De betrokkene heeft in bepaalde gevallen eveneens het recht om de **verwerking** van zijn gegevens te **beperken**. Dit kan bijvoorbeeld wanneer de betrokkene de juistheid van zijn persoonsgegevens betwist.

Verder zal de betrokkene eveneens onder bepaalde voorwaarden het recht hebben om zijn of haar persoonsgegevens in een standaardformaat te ontvangen van de verwerkingsverantwoordelijke. Zo kan de betrokkene de gegevens gemakkelijk overdragen aan een andere leverancier van gelijkaardige dienst (**data portability**).

De betrokkene heeft daarenboven steeds het recht om **bezwaar** te maken tegen de verwerking van zijn of haar persoonsgegevens.

Tot slot heeft iedere betrokkene het recht om een **klacht** in te dienen bij de toezichthoudende overheid wanneer hij of zij meent dat er bij de verwerking van zijn of haar persoonsgegevens een inbreuk gemaakt wordt op de GDPR.

## Data Protection Impact Assessment

Indien men van plan is persoonsgegevens te verwerken en dit een groot risico zou kunnen opleveren voor de betrokkenen, dient men **vóór de verwerking** een data protection impact assessment (DPIA) uit te voeren. Een risico kan zich voordoen bij een grootschalige verwerking van bijzondere categorieën van persoonsgegevens (zoals bijvoorbeeld ras en etnische afkomst) of van gegevens die betrekking hebben op strafrechtelijke veroordelingen. De Europese toezichthouders, waarvan de Belgische Privacycommissie deel uitmaakt, zullen een lijst opstellen van alle soorten verwerkingen waarbij men verplicht is een DPIA uit te voeren.

Wanneer uit de DPIA zou blijken dat de verwerking een hoog risico zou opleveren voor de betrokkenen en de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, dient hij vóór de verwerking, de toezichthoudende autoriteit te raadplegen. Deze zal dan binnen een termijn van 8 weken schriftelijk advies verstrekken.

## Register van de verwerkingsactiviteiten

De huidige verplichting om alle geheel of gedeeltelijk geautomatiseerde gegevensverwerkingen aan te geven bij de Privacycommissie zal geschrapt worden.

Vanaf het moment waarop de GDPR van toepassing wordt op 25 mei 2018, zullen de meeste ondernemingen een **geschreven of elektronisch register** moeten bijhouden van alle verwerkingsactiviteiten die onder hun verantwoordelijkheid gebeuren, het zogenaamde **register van de verwerkingsactiviteiten**.

## Sancties

In eerste instantie zal de toezichthoudende autoriteit **corrigerende maatregelen** voorzien bij overtredingen van de GDPR. Hiervoor kunnen de volgende maatregelen gesteld worden ten opzichte van de verwerkingsverantwoordelijke en/of verwerker: het geven van een waarschuwing of een berisping, het dwingen om verzoeken in te willigen, opdracht geven om persoonsgegevens te wissen of te wijzigen, opdragen om verwerkingen in overeenstemming te brengen met de bepalingen van de GDPR, het verplichten om melding te maken van een inbreuk in verband met persoonsgegevens aan de betrokkene, het opleggen van tijdelijke of definitieve verwerkingsbeperkingen, gegevensstromen naar landen buiten de EU verbieden.

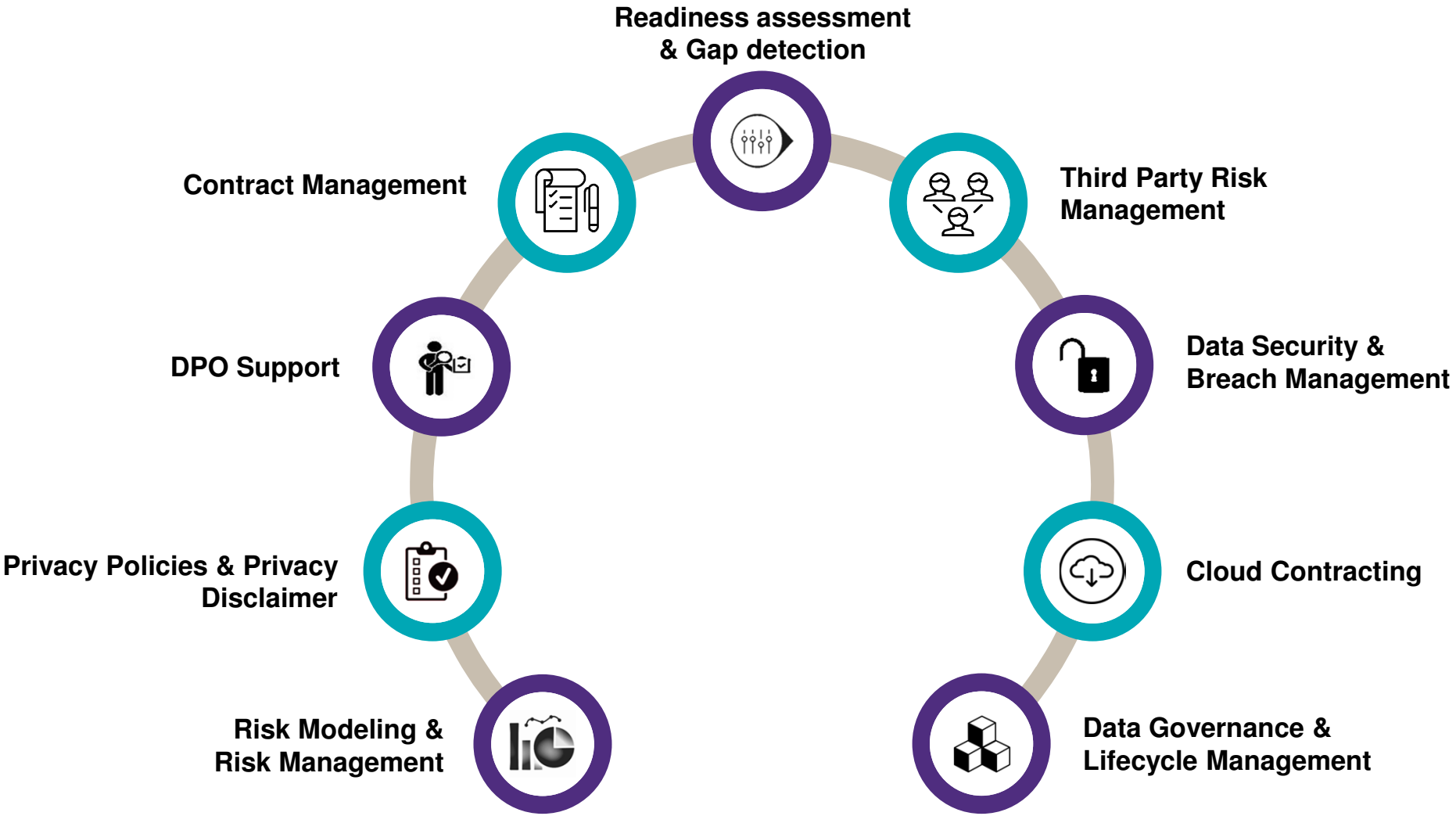
Daarnaast kunnen er **boetes** opgelegd worden aan de verwerkingsverantwoordelijke en/of de verwerker. Er kan een boete opgelegd worden tot 10 miljoen Euro of 2% van de totale wereldwijde jaaromzet indien er een inbreuk is op de verplichtingen van de verwerkingsverantwoordelijke en/of de verwerker.  Bij inbreuken op de algemene beginselen inzake gegevensbescherming of de rechten van de betrokkenen, kan de boete oplopen tot 20 miljoen Euro of 4% van de totale wereldwijde jaaromzet.

## Meldplicht inbreuk

Indien een inbreuk op de persoonsgegevens heeft plaatsgevonden, dient de verwerkingsverantwoordelijke deze **binnen de 72 uur** aan de bevoegde toezichthoudende overheid te melden, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Daarnaast moet de verwerkingsverantwoordelijke de inbreuk **ook melden aan de betrokkene** wanneer de inbreuk waarschijnlijk een hoog risico inhoudt.

# Onze diensten



## Conclusie

Aangezien de GDPR heel wat nieuwe verplichtingen voor uw organisatie met zich meebrengt, verdient het de aanbeveling alvast te onderzoeken welke persoonsgegevens er binnen uw onderneming worden verwerkt, waar deze vandaan komen en met wie u bepaalde gegevens deelt. Hierbij dient u ook te bepalen op welke rechtsgrond u zich beroept voor elke concrete verwerking.

Bij Grant Thornton brengen we al uw uitdadingen rond gegevensbescherming in kaart en bezorgen we u een heldere roadmap zodat we samen met u kunnen werken aan GDPR compliance. U kan een beroep doen op ons team van experten  dat bestaat uit juristen, Business Risk adviseurs en IT adviseurs.

## Our Great Team


Sarah De Ridder
Business Risk Advisor

Sofie Nauwelaerts
Jurist

Ellen Van Ingelgem
Jurist

Timothy Vermeiren
IT Advisor & DPO

Geoffrey Serrien
Business Risk Advisor

**info.gdpr@be.gt.com**