Het waarom en het hoe van de GDPR.

advocaten
Vandebroeck - De Rieck - Verstraeten

Inhoudstafel

Introductie

25 mei 2018 de dag waarop het lijkt dat Europa zich gaat moeien met de wijze waarop wij persoonsgegevens behandelen. De opmerking is niet helemaal correct, maar wel correct is dat zeker de laatste maanden het besef gegroeid is dat onze gegevens belangrijk zijn.

De General Data Protection Regulation of kortweg GDPR heet in het Nederlands Algemene Verordening Gegevensbescherming of AVG. In deze tekst zullen we het gemakkelijkheidshalve bij de Engelse afkortingen houden die vaak beter gekend zijn dan de Nederlandstalige versie ervan.

De bedoeling van de tekst is om op een bevattelijke manier uit te leggen waarom de GDPR nuttig en nodig is, wat de grote principes zijn en vooral welke (minimale) acties je als ondernemer moet ondernemen.

Het is hierbij zeker niet de bedoeling om elk onderwerp van de GDPR volledig en integraal te behandelen. De tekst wil wel een tool zijn waarmee elke ondernemer door het brede werkveld van de GDPR kan fietsen, waardoor hij kan nagaan in hoeverre actie vereist is.

Deel 1

Op wie en op wat is de GDPR van toepassing?

1. Waarover gaat dit eigenlijk en voor wie is het bedoeld?

Eenieder die de actualiteit enigszins volgt, weet dat data of met andere woorden persoonsgegevens het nieuwe zwarte goud zijn geworden. Onze individuele persoonsgegevens zijn elk afzonderlijk niet zo belangrijk, maar de organisaties die erin slagen om massaal veel van dergelijke persoonsgegevens te verzamelen en te combineren, zijn er op korte tijd in geslaagd een totaal nieuw economisch model uit te bouwen. We kunnen eenvoudig verwijzen naar Facebook, Amazon, airbnb en vele andere ondernemingen wiens slagkracht in essentie berust op het verzamelen en beheersen van gigantisch veel persoonsgegevens. Sterker nog, onze persoonsgegevens worden blijkbaar gebruikt voor minder voor de hand liggende activiteiten, zoals het uitwerken van een gepersonaliseerd aanbod op basis van de voorkeuren die we (meestal onbewust) digitaal hebben achtergelaten, tot het beïnvloeden van verkiezingen. Wie de persoonsgegevens beheerst, beheerst de markt (en de politiek).

Aan de andere kant van het spectrum staan alle individuen, bij wie stilaan toch het besef groeit dat enige “digitale hygiëne” misschien toch wel aangewezen is of dat het, anders gezegd, misschien niet zo verstandig is om je ganse leven op Instagram of Facebook te gooien. Om dan verbaasd op te kijken als je wordt afgewezen voor een job op basis van hetgeen op je Facebookprofiel te vinden is of plots geconfronteerd te worden met ransomware omdat je securitybeleid nogal laks bleek.

Kortom, de GDPR wil een (wettelijk en Europees) kader bieden waarbinnen onze persoonsgegevens kunnen verzameld en verwerkt worden. Dit kader is er zowel voor de onderneming die persoonsgegevens gebruikt als voor het individu wiens persoonsgegevens worden gebruikt. Het geeft aan beide zowel rechten als verplichtingen.

Zo is meteen ook de tweede vraag beantwoord: de GDPR is van belang voor zowat iedereen! De ondernemer die nu eenmaal niet kan zonder persoonsgegevens (ook al is hij geen Facebook), en het individu dat vooral rechten put uit de nieuwe regeling.

Dus, concreet?

Ben je ondernemer, besef dan dat je meer persoonsgegevens verwerkt dan je op het eerste gezicht zou denken en dat dit niet langer vrijblijvend kan. Besef dan ook dat diegenen wiens persoonsgegevens je verwerkt, steeds kritischer worden en dat je hun persoonsgegevens moet beschermen. Kortom, de GDPR is een reden om wat je doet te analyseren en een opportuniteit om je als onderneming te profileren.

Ben je een burger, besef dan dat je persoonsgegevens heel belangrijk zijn, gooi ze niet te grabbel en bekijk kritisch wat ermee gebeurt.

2. De GDPR is nieuw, en toch weer niet …

Wellicht is een eerste reactie op de GDPR eerder afwijzend en wordt dit bekeken als weer iets nieuws dat weer eens door Europa wordt opgelegd.

De redenering is te begrijpen, maar ze is niet juist. Vele regels die worden opgelegd door de GDPR bestaan reeds in België en zijn met name vervat in de Wet ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Deze wet is ook gekend als de Privacywet van 8 december 1992, maar bleef in vele gevallen dode letter.

De wet werd niet alleen nauwelijks toegepast, ze was ook echt wel aan vernieuwing toe. Allerlei technologische en grensoverschrijdende vernieuwingen, in combinatie met de enorme toename en het gemak waarmee persoonsgegevens worden verspreid, maakten een nieuwe Europese regeling noodzakelijk.

De Algemene Verordening Gegevensverzameling is vanaf 25 mei 2018 meteen van toepassing in alle Europese landen. Het is evenwel meer dan het louter opfrissen van hetgeen reeds vroeger bestond.
De belangrijkste vernieuwingen hebben te maken met het duidelijker omschrijven van een aantal rechten en verplichtingen, de introductie van een DPO en een uitgebreid sanctiemechanisme.

Deze verschillende aspecten worden verder in dit e-book beschreven.

Dus concreet?

Wake up! De verwerking van persoonsgegevens was voorheen ook reeds gereglementeerd, maar was allicht niet uw eerste zorg. Door de invoering van de GDPR en door de gewijzigde tijdsgeest, kan u dit niet langer negeren. Zoals voorheen reeds beschreven, het is allicht een opportuniteit voor uw onderneming en zo niet moet u misschien denken aan het sanctiemechanisme dat nu wordt ingevoerd.

3. Who is who and what is what?

De GDPR introduceert een aantal nieuwe begrippen. Neem de moeite om deze even te overlopen, vermits ze meteen veel verduidelijken over het toepassen van de GDPR.

- ✔ **Gegevensbeschermingsautoriteit**: de opvolger van de huidige Privacycommissie die waakt over de toepassing van de GDPR.

- ✔ **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Dit is dus echt wel zeer breed: elk gegeven dat ons toelaat om een natuurlijke persoon (dus geen rechtspersoon) direct of indirect te identificeren valt hieronder. Uiteraard gaat het om een naam, een telefoonnummer, een e-mailadres, enz. Het gaat echter ook over elk element dat kenmerkend is voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van een natuurlijke persoon.
  Kortom: alles wat direct of indirect naar een natuurlijke persoon leidt, is een persoonsgegeven. Dus ook documenten, contracten, IP-adressen, camerabeelden, locatiegegevens, …

- ✔ **Verwerkingsverantwoordelijke**: elke onderneming, overheid of organisatie die beslist welke persoonsgegevens ze verzamelt en met welk doel ze dat doet. Kortom: eenieder die persoonsgegevens verwerkt en dat is zowat iedereen.

- ✔ **Verwerker**: elke onderneming, overheid of organisatie die persoonsgegevens verwerkt in opdracht van een verwerkingsverantwoordelijke. In tegenstelling tot de vorige categorie beslist deze niet zelf welke persoonsgegevens ze verzamelt en waarom.

- ✔ **Verwerking**: elke actie waarbij persoonsgegevens worden gebruikt, al dan niet geautomatiseerd. Denk aan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, aligneren of combineren, afschermen, wissen of vernietigen.
  Kortom: elke keer als je persoonsgegevens verzamelt en gebruikt om welke reden dan ook. Daarbij maakt het geen verschil of je een ouderwetse fichebak gebruikt of de meest geavanceerde software.

- ✔ **Betrokkene**: elke geïdentificeerde of identificeerbare natuurlijke en nog levende persoon. Dus in essentie iedereen die in leven en geen rechtspersoon is en van wie de persoonsgegevens worden verwerkt.

- ✔ **Inbreuk met betrekking tot persoonsgegevens**: elk feit waardoor, per ongeluk of bewust, persoonsgegevens worden vernietigd, verloren gaan, gewijzigd of waarbij ten onrechte toegang wordt verleend tot deze gegevens.
  Kortom: elke inbreuk op de CIA van persoonsgegevens of de Confidentiality, Integrity en Availability.

Dus concreet?

Besef dat er eigenlijk geen ontkomen is aan de GDPR. Zowat elk gegeven met betrekking tot een persoon valt onder de toepassing van de GDPR en zowat elke verwerking ervan. Eigenlijk zijn enkel verwerkingen voor louter persoonlijke of huishoudelijke activiteiten uitgesloten en natuurlijk moet het gaan om natuurlijke personen die nog in leven zijn.

4. Let op: Sommige persoonsgegevens worden als gevoelig beschouwd.

Sommige persoonsgegevens worden door de GDPR als “bijzonder” of “gevoelig” omschreven en er gelden bijkomende verplichtingen voor de verwerking van dergelijke gegevens.

Het gaat meer bepaald om de volgende gegevens:

- ✔ **Gezondheidsgegevens**: alle informatie met betrekking tot de lichamelijke of psychische gezondheid of gegevens met betrekking tot de zorg. Een persoon linken aan het adres van een psychiatrische instelling is al voldoende.

- ✔ **Gegevens met betrekking tot** ras, politieke overtuiging, lidmaatschap van een vakbond, filosofische of religieuze overtuigingen, genetische gegevens en biometrische gegevens.

De verwerking van dergelijke gegevens is in principe verboden. Er bestaan evenwel 10 specifieke uitzonderingen op dit principe, die beperkend moeten worden uitgelegd. Onder meer de uitdrukkelijke toestemming, de verwerking in het kader van het arbeidsrecht en sociale zekerheidsrecht, de noodzaak tot het beschermen van de vitale belangen van de betrokkene, …

- ✔ **Strafrechtelijke gegevens**: alle informatie met betrekking tot strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

Ook de verwerking van strafrechtelijke gegevens is strikt verboden en kan enkel gebeuren onder toezicht van de overheid of indien de verwerking uitdrukkelijk wettelijk is toegestaan en er passende waarborgen voor de betrokkenen zijn voorzien.

Dus concreet?

Kijk goed na of je geen bijzondere of gevoelige gegevens verwerkt. Dit zal overigens sneller het geval zijn dan je denkt. Een sportclub bv. houdt allicht gezondheidsgegevens bij en zal aan de specifieke vereisten moeten voldoen.

Besluit na deel 1.

Kijk na of je onder het toepassingsgebied van de GDPR valt. De kans is heel groot, zodra je onderneming op een of andere wijze persoonsgegevens gebruikt.

Kijk na welke persoonsgegevens je verwerkt en of je die persoonsgegevens verwerkt als een “verantwoordelijke”, dan wel louter als een “verwerker”, dus in opdracht. Het is belangrijk voor je verplichtingen binnen de GDPR.

Maak een lijst van de categorieën van persoonsgegevens die je verwerkt. Deze kunnen uiteraard heel divers zijn. De site van de Belgische Privacycommissie vermeldt volgende mogelijke categorieën:

- ✔ Identificatiegegevens
- ✔ Financiële gegevens
- ✔ Persoonlijke kenmerken
- ✔ Fysieke gegevens
- ✔ Leefgewoonten
- ✔ Psychische gegevens
- ✔ Samenstelling van het gezin
- ✔ Vrijetijdsbesteding en interesses
- ✔ Lidmaatschappen
- ✔ Consumptiegewoonten
- ✔ Woningkenmerken
- ✔ Opleiding en vorming
- ✔ Beroep en betrekking
- ✔ Beeld- en geluidsopnames

Kijk na of de persoonsgegevens die je verzamelt te beschouwen zijn als bijzondere of gevoelige gegevens.

Deel 2

Hoe en waarom je persoonsgegevens kan verwerken volgens de GDPR

Zoals hierboven reeds gesteld: de GDPR is er niet plots gekomen, maar is het resultaat van een streven naar een betere bescherming van onze individuele persoonsgegevens. Een aantal uitgangspunten van de GDPR moeten dan ook vanuit die achtergrond worden bekeken en vooral begrepen. Hierdoor is meteen aangegeven welke houding je als verwerkingsverantwoordelijke moet aannemen tegenover de persoonsgegevens die je verwerkt.

1. Data Protection by design and by default.

Als verantwoordelijke voor de verwerking van persoonsgegevens, moet je kunnen aantonen dat je de nodige technische en organisatorische maatregelen hebt genomen met als doel de principes van de gegevensbescherming op een doeltreffende manier uit te voeren en om de nodige waarborgen in te bouwen ter naleving van de voorschriften van de verordening.

Vooraleer je persoonsgegevens gaat verzamelen, laat staan verwerken, moet je dus de principes van de GDPR erbij halen en ervoor zorgen dat het “design” van je activiteit maximaal correspondeert met die principes.

Je moet deze oefening maken rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en doel van de verwerking en de risico’s voor de rechten en de vrijheden van de betrokkenen.

Verder moet je ervoor zorgen dat alle technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat in beginsel enkel persoonsgegevens worden verwerkt die noodzakelijk zijn voor een specifiek doel. De standaardinstelling of de “default” instelling moet deze zijn waarbij het minste persoonsgegevens worden verzameld.

Dus concreet?

Het gaat niet meer op om zomaar wat persoonsgegevens te verzamelen. Als ondernemer moet je bewust nadenken over welke gegevens je werkelijk nodig hebt en of de wijze waarop je die gegevens verwerkt in overeenstemming is met de basisprincipes van de GDPR. Vandaag moet je die oefening allicht achteraf maken, maar wanneer je diezelfde oefening op voorhand kan maken, wordt het uiteraard makkelijker.

2. Waarom mag ik persoonsgegevens verwerken of nog beter: wat is mijn verwerkingsgrond?

Het is misschien vreemd opkijken, maar je kan niet zomaar persoonsgegevens verwerken, louter omdat je dat interessant vindt. Voor elke (!) verwerking heb je een specifieke verantwoording nodig en de GDPR voorziet 6 en slechts 6 mogelijkheden.

We overlopen even de mogelijke verwerkingsgronden.

✔ **De overeenkomst.**
Om een gekocht product te kunnen leveren, heb ik nu eenmaal een adres nodig. Om de belangen van een cliënt te kunnen verdedigen, heeft de advocaat nu eenmaal vele persoonsgegevens nodig. De verwerking van de persoonsgegevens is dan ook noodzakelijk om de overeenkomst te kunnen uitvoeren. Let wel: als de overeenkomst erin bestaat om een gekocht product te leveren, is dit dus geen grond om nadien aan de klant een promotiefolder op te sturen.

✔ **De wettelijke verplichting.**
De werkgever is verplicht om bepaalde gegevens aan de RSZ mee te delen. De verwerking is dus noodzakelijk om aan een wettelijke verplichting te voldoen.

✔ **De vitale belangen van de betrokkene.**
Nood breekt wet. Wanneer het leven van de betrokkene in gevaar is, kunnen persoons-gegevens worden verwerkt. Dit is echt een uitzonderingssituatie waarbij geen enkele andere verwerkingsgrond mogelijk mag zijn.

✔ **Het algemeen belang en het openbaar gezag**
Dit criterium is vooral van toepassing in de publieke sector en is niet echt relevant voor de private onderneming.

✔ **Het gerechtvaardigd belang.**
In tegenstelling tot de vorige categorie gaat het hier niet om het algemeen belang, maar wel om het eigen belang van de onderneming. De onderneming mag persoonsgegevens verwerken indien die nodig zijn om haar eigen belangen te bewerkstelligen.
Dit lijkt natuurlijk de oplossing, want elke onderneming wil haar eigen belangen bewerk-stelligen. Toch niet, De GDPR voorziet immers heel uitdrukkelijk dat een belangenafweging moet worden gemaakt tussen het eigen belang en de belangen van de betrokkene. Let op dat deze belangenafweging natuurlijk achteraf kan beoordeeld worden en kan leiden tot sancties indien die te licht wordt bevonden.
Voor een aantal sectoren is dit criterium heel belangrijk, onder meer alle vormen van direct marketing, ongevraagde niet commerciële berichten met het oog op goede doelen of politieke campagnes, preventie van fraude en witwas, fysieke veiligheid, historisch weten-schappelijk of statistisch onderzoek, …

Dus concreet?
Wacht nog even en lees dit samen met het volgende stukje.

3. De toestemming.

De aandachtige lezer zal opgemerkt hebben dat onder het vorige nummer slechts 5 van de 6 verwerkingsgronden werden besproken. De zesde verwerkingsgrond, nl. de toestemming is dermate specifiek dat we dit apart behandelen.

Toestemming lijkt de meest belangrijke verwerkingsgrond te zijn. Laat ergens onderaan een vakje "I accept" aanvinken en de zaak is geklaard. Dat is echter onder de nieuwe GDPR niet meer het geval. De toestemming is onderworpen aan specifieke voorwaarden en verleent de betrokkene specifieke rechten, zodat u de toestemming eerder zal willen gebruiken als er geen andere verwerkingsgronden mogelijk zijn.

In de GDPR wordt heel precies beschreven wat we onder toestemming moeten begrijpen.

Het gaat nl. om een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, hetzij door een verklaring, hetzij door een ondubbelzinnige actieve handeling en waaruit blijkt dat de betrokken persoon deze precieze verwerking aanvaardt.

Elk woord in die omschrijving is belangrijk, maar het komt erop neer dat er enkel een toestemming in de zin van de GDPR bestaat als die

- ✔ Geheel vrij is gegeven: de toestemming werd niet afgedwongen en kan op elk ogenblik en even eenvoudig worden ingetrokken zonder sanctie.
- ✔ Geïnformeerd is gegeven: de betrokkene wordt heel duidelijk en in een begrijpelijke taal op de hoogte gebracht van de verwerking.
- ✔ Specifiek is gegeven: de toestemming moet per soort verwerking zijn gegeven, dus geen algemeen "I accept" meer.
- ✔ Ondubbelzinnig zijn gegeven: de betrokkene moet op een actieve manier zijn toestemming hebben gegeven of m.a.w. "zwijgen is toestemmen" telt niet. Dus een Opt In en geen Opt Out!

Op zich zijn dit reeds verregaande voorwaarden, maar het gaat nog verder.

Als ondernemer moet je steeds kunnen bewijzen dat een geldige toestemming werd bekomen, mag je de toestemming niet verbergen in de kleine lettertjes en moet je per specifiek doel een eigen toestemming bekomen. De betrokkene heeft ook uitdrukkelijk het recht om op elk ogenblik zijn toestemming in te trekken en dat moet op een even eenvoudige wijze kunnen gebeuren als het geven van de toestemming.

Indien het gaat om een aanbod van onlinediensten aan een kind, kan dit pas wanneer het kind 16 jaar is. Is het kind jonger dan 16 jaar dan moet je de toestemming van de ouders bekomen!

Dus concreet?

Bepaal welke verwerkingsgrond voor jou het meest geschikt is om te dienen als basis voor het verwerken van de persoonsgegevens.
De meest voor de hand liggende gronden zullen zijn: de overeenkomst, het gerechtvaardigd belang en de wettelijke verplichting.

Toestemming is in tegenstelling tot wat je zou denken, niet het meest evidente. Toestemming is immers onderworpen aan heel strenge voorwaarden en geeft de betrokkene de volledige controle. Meer nog, in de meeste gevallen zal je voor bestaande verwerkingen, na 25 mei 2018 een nieuwe toestemming moeten vragen!

Besluit na deel 2.

Bezin voor je begint. Het is niet meer mogelijk om zomaar persoonsgegevens te verzamelen. Als je denkt aan een commerciële actie waarbij je (uiteraard) persoonsgegevens gebruikt, als je een nieuwe online webwinkel opzet, als je denkt een nieuwe markt aan te boren, … moet je op voorhand nadenken over de persoonsgegevens die je hiervoor echt nodig hebt en hoe je die activiteit het best kan realiseren in overeenstemming met de principes van de GDPR.

Bekijk het zo: wie een huis bouwt, denkt niet aan de verplichtingen inzake isolatie nadat het huis is opgeleverd.

Hierbij is het heel bepalend welke van de 6 verwerkingsgronden (er zijn er geen andere) op die activiteit van toepassing is. Een combinatie is uiteraard perfect mogelijk.

Een advocatenkantoor steunt in eerste instantie op de overeenkomst voor de verwerking van de gegevens van de cliënten, op de wettelijke verplichting om de gegevens van het personeel te verwerken, op de toestemming indien het kantoor die gegevens voor commerciële doeleinden zou willen gebruiken.

Let zeker ook op bij het verwerken van gevoelige gegevens. Dan zijn er immers bijkomende verplichtingen of uitzonderingen.

Deel 3

De beginselen van de GDPR en de rechten van de betrokkene.

We weten intussen dat de GDPR er gekomen is om de verwerking van persoonsgegevens enerzijds te reglementeren en anderzijds te beschermen. Die dubbele functie vinden we terug enerzijds in de basisbeginselen die elke verwerking moet respecteren en anderzijds in de rechten die elke betrokkene heeft. We bespreken beide functies hierna.

1. De basisbeginselen van de GDPR

Onder deel 2 hadden we het over data protection by design and by default of hoe je van tevoren moet nadenken over het inpassen van de GDPR. Daarbij moet je uitgaan van een aantal principes die overigens ook elk afzonderlijk in de GDPR zijn voorzien.

✔ **De verwerking moet rechtmatig, behoorlijk en transparant zijn.**
Dit is eigenlijk de samenvatting van hetgeen onder deel 2 reeds werd besproken. Een verwerking is rechtmatig als je beschikt over de correcte verwerkingsgrond, behoorlijk als ze eerlijk is en transparant als ze duidelijk en begrijpelijk werd uitgelegd.

✔ **De verwerking moet dienen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (doelbinding).**
Je verwerkt persoonsgegevens met een bepaalde bedoeling en dat doel moet je heel precies en uitdrukkelijk kunnen aanduiden. Dit betekent meteen ook dat je die gegevens enkel voor dat precieze doel mag gebruiken. Meer nog, je mag de gegevens enkel gebruiken voor hetgeen in overeenstemming is met de redelijke verwachtingen van de betrokkene.

✔ **De verwerking moet minimaal zijn.**
Om het doel van hierboven te bereiken heb je bepaalde persoonsgegevens nodig. De minimale verwerking houdt in dat je enkel die gegevens mag verzamelen die je absoluut nodig hebt, niet meer en niet minder. Meteen een moeilijke oefening.

✔ **De verwerking moet accuraat zijn.**
Hiermee wordt bedoeld dat je gegevens juist moeten zijn en actueel. Of m.a.w. je moet systemen opzetten om je gegevens regelmatig bij te werken en ervoor te zorgen dat er geen fouten insluipen. De betrokkenen zelf hebben trouwens het recht om hun gegevens te verbeteren, zoals later nog wordt uitgelegd.

✔ **De verwerking moet beperkt zijn in de tijd.**
Je moet aangeven hoelang je de gegevens bewaart. Dat kan bv. zijn 1 jaar, of zolang het nodig is om de overeenkomst uit te voeren, of zolang de wetgever mij verplicht om gegevens bij te houden, … Het mag evenwel niet onbeperkt zijn en dus moeten die gegevens na de aangegeven periode worden verwijderd of anoniem gemaakt. Let op: ook een back up is natuurlijk een bestand met gegevens en valt onder alle GDPR verplichtingen.

✔ **De verwerking moet de integriteit en vertrouwelijkheid garanderen.**
Als verwerkingsverantwoordelijke moet je de passende technische en organisatorische maatregelen nemen om ervoor te zorgen dat je gegevens niet verloren gaan (al dan niet vrijwillig), beschadigd of vernietigd worden.

✔ **Verantwoordingsplicht.**
Dit is een belangrijk principe: de ondernemer die de gegevens verwerkt, is hiervoor verantwoordelijk en moet te allen tijde kunnen aantonen dat hij zich houdt aan de verplichtingen en principes van de GDPR.

Dus concreet?

De manier waarop je momenteel met persoonsgegevens omgaat, zal allicht eerder praktisch en organisch gegroeid zijn en allicht heb je dit louter vanuit je eigen perspectief gedaan. Welnu, je eigen perspectief wordt vanaf nu dat je verantwoordelijk bent en verantwoording moet kunnen afleggen voor het naleven van deze principes. De moeite waard dus om ze even in de weegschaal te leggen.

2. De rechten van de betrokkene.

Achter de persoonsgegevens zit uiteraard altijd een levende natuurlijke persoon. Die persoon krijgt in de GDPR heel duidelijke en specifieke rechten toebedeeld. We worden allemaal ook meer en meer bewust van het belang van onze gegevens en de kans wordt dus groter dat die persoon ook effectief zijn of haar rechten gaat gebruiken. Je moet hier dus rekening mee houden.

De rechten zijn op zich vrij duidelijk, ze in de praktijk inbouwen kan soms iets complexer zijn. We overlopen ze aan de hand van drie logische en opeenvolgende fases in het verloop van de gegevensverwerking.

Bij aanvang van de werking:

✔ **Het recht om geïnformeerd te worden.**
In de aanvangsfase moet je de betrokkene informeren omtrent het feit dat zijn persoonsgegevens worden verwerkt en van de modaliteiten ervan. Gaat het om gegevens die je zelf rechtstreeks bij de betrokkene hebt bekomen, dan moet je dit op het ogenblik zelf meedelen, gaat het om gegevens die je via derden hebt bekomen, dan moet je dit binnen een redelijke termijn, maar uiterlijk binnen de maand meedelen.
Wat je moet meedelen, wordt eveneens voorzien: het gaat om de doeleinden, de verwerkingsgrond(en), de duurtijd, de mededeling aan derden, …

✔ **Het recht op verzet.**
Als je de betrokkene informeert omtrent de verwerking van zijn persoonsgegevens heeft hij het recht om hiertegen verzet aan te tekenen of m.a.w. bezwaar in te dienen.
Dit bezwaar kan te maken hebben met de specifieke situatie waarin de betrokkene zich bevindt of kan altijd in geval van verwerking met het oog op direct marketing.

Een bijzondere bepaling hier is het verzet tegen profilering, of een volledig geautomatiseerde verwerking waaraan voor de betrokkene rechtsgevolgen zijn verbonden. Overigens, het verzet kan altijd worden uitgeoefend, dus ook in de volgende fases.

Tijdens de verwerking:
Nadat de eerste horde is genomen, heeft de betrokkene ook specifieke rechten tijdens de verwerking van zijn persoonsgegevens.

✔ **Recht op toegang en inzage.**
De betrokkene kan op elk ogenblik vragen of zijn gegevens worden verwerkt, welke gegevens worden verwerkt, waarom en onder welke modaliteiten.
Merk op dat de GDPR een heel precieze lijst bevat van de informatie die moet worden meegedeeld.

Onder dit aspect wordt het recht geplaatst om (gratis) een kopie te bekomen van alle persoonsgegevens die worden verwerkt

✔ **Recht op verbetering.**
Dit behoeft weinig uitleg: de betrokkene kan (bv. na inzage) eisen dat foute gegevens worden verbeterd, onvolledige gegevens worden aangevuld.

✔ **Recht op overdraagbaarheid.**
De betrokkene heeft het recht om te vragen dat zijn gegevens, zonder enige hinder, worden overgedragen aan een andere partij (bv. bij overgang naar een andere provider). Let wel, dit recht bestaat enkel voor gegevens die zelf werden verstrekt, wanneer de verwerking steunt op toestemming of overeenkomst en wanneer de verwerking gebeurt op geautomatiseerde procedés.

✔ **Recht op beperking.**
In bepaalde gevallen kan de verwerking "on hold" worden gezet, nl. gedurende de tijd die nodig is om een vraag van de betrokkene te onderzoeken of indien men gegevens wil behouden die normaal zouden worden gewist. De GDPR voorziet hier opnieuw heel specifieke toepassingsvoorwaarden.

Bij het einde van de verwerking.
Zoals eerder reeds beschreven, mogen persoonsgegevens slechts een bepaalde tijd worden bewaard. Daarvoor heeft de betrokkene evenwel het recht om zijn gegevens te laten wissen (de GDPR voorziet 6 specifieke gevallen) en heeft hij het recht om vergeten te worden. Met dit laatste wordt bedoeld dat de verwerkingsverantwoordelijke al het mogelijke moet doen om ervoor te zorgen dat iedereen die je gegevens heeft ontvangen ervoor zorgt dat elke link, kopie of reproductie wordt verwijderd.

Hierdoor komt er natuurlijk een einde aan de verwerking.

Dus concreet?

Iedereen is baas over zijn of haar eigen persoonsgegevens. Dit was voor de GDPR eigenlijk al het geval, maar wordt nu nog meer expliciet gemaakt. Diegene die de persoonsgegevens verwerkt, moet daarmee rekening houden.

Besluit na deel 3.

Diegene wiens persoonsgegevens worden verwerkt heeft rechten, diegene die persoonsgegevens verwerkt moet op elk ogenblik kunnen verantwoorden dat die verwerking in overeenstemming is met de beginselen en rechten zoals hierboven uiteengezet.

In essentie: de verwerking van persoonsgegevens is enkel mogelijk als dit gebeurt in volledige openheid en transparantie en wanneer die op elk ogenblik rekening houdt met de rechten van de betrokkene. De systemen die gebruikt worden bij die verwerking moeten dit mogelijk maken en garanderen.

Deel 4

De expliciete verplichtingen van de verwerkingsverantwoordelijke.

In de vorige delen ging het vooral over de grote principes, over rechten en plichten, over de verwerkings-verantwoordelijke die verantwoording moet kunnen afleggen, kortom over data protection by design and by default. In de GDPR worden echter ook een aantal heel duidelijke verplichtingen en expliciete maatregelen opgelegd. Elk van deze verplichtingen is op zich weer een veruitwendiging van de grote principes, rechten en plichten die we in de vorige delen hebben besproken.

1. Het opmaken van een verwerkingsregister.

Zoals de naam het al aangeeft, is dit een fysiek bestaand register (op papier, elektronisch, …) waarin alle verwerkingen worden beschreven.

In theorie rust deze verplichting niet op KMO's met minder dan 250 werknemers, maar "de uitzonderingen op deze uitzondering" maken dat zowat elke KMO, ongeacht het aantal werknemers, er toch weer onder valt.

De GDPR legt geen vorm op en eenieder is dus vrij om het register naar eigen goeddunken op te stellen, met dien verstande dat de GPPDR wel een aantal categorieën van gegevens opsomt die in het register moeten zijn opgenomen.

Samengevat gaat het om de volgende gegevens:

- ✔ Contactgegevens van de verantwoordelijke(n) en de DPO
- ✔ De doeleinden van de verwerking
- ✔ Categorieën van betrokkenen en persoonsgegevens
- ✔ Lijsten van iedereen aan wie de gegevens worden doorgeven (binnen en buitenland)
- ✔ De termijn waarbinnen de gegevens worden gewist
- ✔ Een beschrijving van alle technische en organisatorische maatregelen

In de praktijk is dit meestal een (al dan niet uitgebreid) Excelbestand waarin eigenlijk het resultaat wordt genoteerd van alle analyses en vragen die worden beschreven in deel 2 en 3.

2. Het opstellen en publiceren van een privacy policy.

Hoger hebben we er reeds op gewezen dat de betrokkene moet geïnformeerd worden over de verwerking van zijn persoonsgegevens.

De meest aangewezen manier om dit te doen is via een privacy policy die bij het contract kan gevoegd worden of op de website gepubliceerd wordt.

De gegevens die in deze privacy policy moeten worden opgenomen, zijn eveneens het resultaat van alle analyses en vragen die worden beschreven in deel 2 en 3. Het gaat dus om het antwoord op de vragen wie de verantwoordelijke is, welke gegevens worden verwerkt en met welk doel, op basis van welke rechtsgrond, hoelang de bewaringstermijn is, wat de rechten van de betrokkene zijn, …

Vanuit het eveneens reeds eerder beschreven principe van transparantie, moet deze privacy policy goed leesbaar, duidelijk en overzichtelijk zijn. Of inderdaad, geen “kleine lettertjes” meer. Worden bepaalde gegevens verwerkt op basis van toestemming, dan moet hieraan bijzondere aandacht geschonken worden en moet deze toestemming afzonderlijk verkregen worden, zoals hoger reeds beschreven.

3. Het opstellen van een verwerkersovereenkomst.

Voor de verwerking van bepaalde persoonsgegevens doe je noodzakelijkerwijze beroep op een andere firma, die meer gespecialiseerd is en aan wie je dus de gegevens doorgeeft. Het meest voor de hand liggende voorbeeld is het sociaal secretariaat aan wie je de persoonsgegevens van het personeel doorgeeft om de lonen te laten berekenen.

De GDPR legt de verplichting op om erover te waken dat die verwerker zelf voldoende garanties geeft opdat de verwerking conform de voorschriften van de GDPR zou zijn. De GDPR bevat trouwens zelf een aantal artikelen die specifiek op de verwerker van toepassing zijn, zodat het ook voor deze oppassen geblazen is. Het gaat onder meer om de verplichting om zelf een contract op te stellen met sub-verwerkers of de verplichting om de verantwoordelijke te informeren bij een inbreuk.

Ook de inhoud van de verwerkersovereenkomst wordt uitdrukkelijk beschreven in de GDPR. In niet minder dan 7 bepalingen worden een aantal maatregelen vastgelegd die er moeten op toe zien dat de verwerker enkel handelt op basis van schriftelijke instructies en dat hij alle waarborgen verstrekt zodat de verwerker en zijn medewerkers GDPR compliant zijn.

4. Een functionaris voor gegevensbescherming (of DPO) aanstellen.

De GDPR introduceert een nieuwe functie, met name de “functionaris voor gegevensbescherming”, die wij meestal aanduiden met de Engelstalige omschrijving van Data Protection Officer of DPO.

De opdracht van de DPO bestaat erin om binnen de onderneming toe te zien op de naleving van de voorschriften van de GDPR en uiteraard ook om de onderneming bij de te staan, bv. bij het opstellen van het verwerkingsregister of het uitvoeren van een DPIA (zie hieronder). De DPO kan intern of extern worden aangesteld, maar staat wel steeds onafhankelijk tegenover de onderneming. De DPO is onder meer het contactpunt voor de toezichthoudende autoriteit.

Let wel, niet iedere ondernemer moet een DPO aanstellen. Dit is enkel verplicht in de volgende drie gevallen.

- ✔ Alle openbare overheden en openbare organismen, behalve bij de uitoefening van hun rechterlijke taken.
- ✔ Een onderneming die hoofdzakelijk belast is met verwerkingen die omwille van hun aard, omvang of doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen.
- ✔ Een onderneming die hoofdzakelijk is belast met de grootschalige verwerking van bijzondere categorieën van gegevens of van persoons-gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

Elk van deze begrippen is nogal vaag en kan leiden tot verschillende interpretaties. In elk geval moet het gaan om ondernemingen voor wie de verwerking hun core business is en waar die verwerking betrekking heeft op grote categorieën van betrokkenen en gegevens.

5. Het uitvoeren van een DPIA of Data Protection Impact Assessment.

Geef toe, DPIA is makkelijker uit te spreken dan de Nederlandse versie, nl. “Gegevensbeschermings-effectbeoordeling” en we houden het dan ook op de Engelse afkorting om deze nieuwe verplichting te omschrijven.

Het komt erop neer dat de verwerkingsverantwoordelijke, in situaties die waarschijnlijk een “bijzonder hoog risico” inhouden voor de rechten en vrijheden van de betrokkene, een risicoanalyse moet uitvoeren en dit uiteraard vooraleer de verwerking kan beginnen. Er wordt in het bijzonder verwezen naar verwerkingen die gebeuren met gebruik van nieuwe technologieën. De GDPR voorziet trouwens ook een aantal situaties waarbij een dergelijke DPIA verplicht moet worden uitgevoerd en ook hier zijn er voorschriften die bepalen wat minimaal de inhoud van deze analyse moet zijn.

Uiteraard kan deze analyse leiden tot het nemen van bepaalde maatregelen om de impact voor de betrokkenen te verminderen en moet in bepaalde gevallen de problematiek worden voorgelegd aan de toezichthoudende overheid.

6. De persoonsgegevens beveiligen.

Het is al duidelijk gemaakt dat je als verwerkingsverantwoordelijke of als verwerker, de verantwoordelijkheid draagt voor de beveiliging van de gegevens en dat je dit ook moet kunnen aantonen.

De GDPR voorziet uitdrukkelijk dat je alle passende technische en organisatorische maatregelen moet nemen om je gegevens te beveiligen en die maatregelen moeten in overeenstemming zijn met de stand van de techniek en de kostprijs.

Elke onderneming moet dus voor zich uitmaken hoe groot het risico is dat gegevens worden vernietigd, verloren gaan, gewijzigd worden, gehackt worden. Elke onderneming zal dus ook voor zich moeten uitmaken welke gevolgen een dergelijke data breach kan hebben voor de onderneming en de betrokkenen.

Heel belangrijk hierbij is ervoor te zorgen dat deze analyses en maatregelen goed gedocumenteerd zijn, bv. in een verwerkingsregister of een DPIA.

Besluit na deel 4.

Elke verwerkingsverantwoordelijke of verwerker moet de grote principes van de GDPR in de praktijk omzetten. Het resultaat van de denkoefeningen en analyses die beschreven worden in de delen 3 en 4 -, moet zijn weg vinden naar een verwerkingsregister (wat een louter intern document is), een Privacy Policy (wat een extern document is) of een DPIA. De ondernemer moet nakijken of de aanstelling van een DPO nodig is en dan uiteraard de aanbevelingen van deze DPO opvolgen. De ondernemer moet ervoor zorgen dat de beveiliging van zijn gegevens op het niveau is dat van een dergelijke ondernemer mag verwacht worden. Het is dus niet aanvaardbaar (en overigens ook onverstandig) om geen maatregelen genomen te hebben. Afhankelijk van de aard van de onderneming gaat dit overigens verder dan het installeren van een basis antivirusprogramma. Er kan ook verwacht worden dat interne procedures worden opgezet om de elektronische en fysieke veiligheid te waarborgen.

Deel 5

Wat als het fout gaat?

De GDPR laat het niet bij mooie woorden alleen. Er zijn nieuwe verplichtingen en sancties.

1. Het verplicht melden van een inbreuk op de data.

Elke inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens moet gemeld worden.

Vooreerst moet je als onderneming elke inbreuk documenteren en opnemen (bv in het verwerkingsregister): wat was de oorzaak van het probleem, welke persoonsgegevens zijn betrokken, welke maatregelen zijn er genomen?

Vanaf het ogenblik dat er een risico is voor de rechten van de betrokkene moet je het ook melden, waarbij er dan weer twee fases zijn.

✔ **Melding aan de gegevensbeschermingsautoriteit (de vroegere Privacycommissie).**
Als verwerkingsverantwoordelijke moet je elk gegevenslek melden aan de toezichthouder, tenzij het niet waarschijnlijk is dat het lek een risico inhoudt voor de rechten en de vrijheden van de betrokkene.

Deze melding moet bovendien zonder onredelijke vertraging gebeuren en alleszins binnen de 72 uur.

Minstens moet volgende informatie worden meegedeeld:
- De aard van de inbreuk, de categorieën van betrokkenen en het aantal betrokkenen en bestanden
- Naam en contactgegevens van de DPO of ander contact
- De waarschijnlijke impact van de inbreuk
- De maatregelen genomen om de inbreuk en de impact ervan te remediëren

✔ **Melding aan de betrokkenen zelf.**
Wanneer de inbreuk waarschijnlijk een “hoog risico” inhoudt voor de rechten en vrijheden van de betrokkenen, dan moeten zij eveneens op de hoogte gebracht worden en dit moet bovendien “onverwijld” gebeuren.

Deze melding moet eveneens de hogervermelde gegevens bevatten, maar moet bovendien in een duidelijke en eenvoudige taal zijn opgesteld.

Merk op dat de gegevensbeschermingsautoriteit je achteraf nog kan verplichten om de inbreuk te melden.

Het zal er natuurlijk op aan komen om te bepalen of er al dan niet sprake is van een hoog risico, want de melding aan alle betrokkenen, bv. al uw klanten, is een verregaande maatregel. Het ligt voor de hand dat er vooral moet afgewogen worden hoe gevoelig de gegevens zijn en vooral hoe snel ze er kunnen toe leiden dat individuen kunnen geïdentificeerd worden.

2. De mogelijkheid van verhaal of om een klacht in te dienen.

Iedereen die meent dat zijn rechten worden geschonden, heeft het recht om bij de gegevens-beschermingsautoriteit een “doeltreffende voorziening” of m.a.w. een klacht in te dienen. Deze gegevensbeschermingsautoriteit beschikt dan over een eigen arsenaal van sancties die hierna worden besproken.

Houd er ook rekening mee dat een betrokkene die meent dat zijn rechten worden geschonden, ook voor de gewone rechtbank de stopzetting of een schadevergoeding kan eisen. De verwerkings-verantwoordelijke of de verwerker zal dan moeten aantonen dat hij geen enkele fout heeft begaan om aan veroordeling te ontsnappen.

3. De gegevensbeschermingsautoriteit kan een sanctie opleggen.

In tegenstelling tot de huidige privacycommissie kan de gegevensbeschermingsautoriteit op basis van een klacht of zelf sancties opleggen. Als onderneming bent u trouwens verplicht om uw medewerking te verlenen bij een eventueel onderzoek.

De mogelijke sancties zijn heel divers. Het gaat bv. om volgende sancties:

- ✔ Een waarschuwing of een berisping
- ✔ De verplichting om in te gaan op de klacht van een betrokkene
- ✔ De verplichting om u te conformeren aan de GDPR
- ✔ Het opschorten van een bepaalde verwerkings-activiteit
- ✔ Een boete die, afhankelijk van de inbreuk, kan oplopen tot 2% of 4% van de jaaromzet

Besluit na deel 5.

We weten reeds dat het verzamelen en verwerken van persoonsgegevens dus niet vrijblijvend meer is. Dankzij de GDPR kan de gegevensbeschermings-autoriteit zelf of kan de betrokkene een procedure opstarten waarbij u bepaalde sancties en boetes kunnen worden opgelegd. De betrokkene die meent dat zijn rechten geschonden zijn, kan zich ook tot de gewone rechtbank wenden om schade-vergoeding te bekomen. Het is best om dat in het achterhoofd te houden.

Deel 6

Hoe pak je dit nu concreet aan?

De GDPR vraagt van de ondernemer een nieuwe mindset over persoonsgegevens en over hoe met die gegevens om te gaan. Die nieuwe mindset kan behoorlijk ver gaan en voor de bedrijven bij wie het verwerken (verhandelen) van persoonsgegevens de core business uitmaakt, heeft de GDPR een enorme impact.

Voor de gemiddelde Vlaamse KMO betekent dit vooral dat een aantal stappen moeten worden genomen, die zullen leiden tot een aantal concrete acties.

1. Identificeer!

Bepaal of je een verwerkersverantwoordelijke bent en met welke andere bedrijven je de persoonsgegevens deelt en die dus allicht verwerkers zullen zijn. Het gaat meestal om het sociaal secretariaat, de software-leveranciers, het communicatiebedrijf dat je mailings verzorgt, de leverancier die je klantenkaarten beheert, …

Bepaal welke categorieën van betrokkenen je hebt. Denk hierbij uiteraard aan je personeel, je klanten, je prospecten, je sollicitanten, …

Bepaal welke categorieën van persoonsgegevens je verzamelt. Denk hierbij aan identificatiegegevens, contactgegevens, financiële gegevens, … kijk in het bijzonder na of je gevoelige persoonsgegevens verzamelt.

Bepaal met welk specifiek doel je persoonsgegevens verwerkt en op basis van welke rechtsgrond.
Bepaal welke (IT-)maatregelen, procedures, ... je hebt om de persoonsgegevens te beschermen.

2. Stel een privacyverklaring op!

De privacyverklaring is je uithangbord. Hier leg je in een duidelijke en begrijpelijke taal uit hoe je conform de regelgeving van de GDPR handelt en hoe je de rechten van de betrokkene respecteert.

Een uithangbord is er om gezien te worden. Je privacy-verklaring moet dus meegedeeld worden op alle mogelijk manieren, zodat de betrokkenen er onmiddellijk kennis kunnen van hebben.

3. Stel een verwerkingsregister op!

Het verwerkingsregister is je intern logboek, waarin je voor jezelf documenteert hoe je conform de regelgeving van de GDPR handelt en hoe je de rechten van de betrokkene respecteert. Dit register is geen statisch gegeven, maar wordt aangevuld bij elke nieuwe verwerking, bij elke inbreuk, … Het is van essentieel belang, zeker op het ogenblik waarop je zal gevraagd worden om de naleving van de GDPR voorschriften aan te tonen.

4. Stel een DPO aan en voer een DPIA uit!

Het effectief aanstellen van een Data Protection Officer of het uitvoeren van een Data Protection Impact Assessment is slechts in specifieke gevallen verplicht.

5. Stel de nodige overeenkomsten op!

Met iedereen die de persoonsgegevens verwerkt, moeten specifieke overeenkomsten worden opgesteld. Dit is zowel voor het eigen personeel met wie je een addendum aan de arbeidsovereenkomst toevoegt, als voor elke derden firma met wie je een verwerkersovereenkomst afsluit.

6. Data protection by design and by default!

Denk bij dit alles na over de persoonsgegevens en over de wijze waarop je die verwerkt. Uiteindelijk is het de bedoeling om niet meer persoonsgegevens te verwerken dan je strikt nodig hebt en uiteraard conform de principes van de GDPR. Zeker als het gaat om een nieuwe verwerkingsactiviteit is het zinvol om de oefening op voorhand te maken.

Besluit

Via de invoering van de GDPR wil de wetgever een nieuwe mindset bewerkstelligen bij elkeen die persoonsgegevens verwerkt en bij elkeen wiens persoonsgegevens worden verwerkt. Het vraagt alleszins om een proactief beleid waarbij met open vizier naar de betrokkenen wordt toegestapt.

De grote principes zijn duidelijk, het komt er nu op aan om deze in de praktijk om te zetten en de analyses te maken die in dit e-book worden beschreven.

Voor de concrete uitwerking van uw GDPR dossier, het aanvragen van modellen kan u steeds contact opnemen met het kantoor en de auteur, mr Jan De Rieck.

De auteur: Mr Jan De Rieck

Mr Jan De Rieck is stichtend advocaat-vennoot van het advocatenkantoor Vandebroeck-De Rieck-Verstraeten, gekend onder advocaten-leuven.be. Het kantoor streeft ernaar om uw juridische vragen op een gespecialiseerde, klantvriendelijke en resultaat-gerichte manier aan te pakken. Dit e-book is een voorbeeld van die filosofie. Mr Jan De Rieck is gespecialiseerd in ondernemingsrecht in de brede zin en in insolventierecht. Hij is advocaat sinds 1991 en maakt sinds september 2010 ook deel uit van de Orde van advocaten te Leuven. Sinds september 2016 is hij stafhouder van de Orde van advocaten te Leuven. Hij volgde ook met succes de opleiding tot Certified Data Protection Officer en is dus perfect geplaatst om u te begeleiden bij de concrete invulling van de GDPR verplichtingen in uw onderneming.

Meer info en concrete bijstand inzake de GDPR:

Kantoor Leuven
Vaartstraat 68-70, 3000 Leuven

Kantoor Heist-op-den-Berg
Dorpsstraat 72A, 2221 Heist-op-den-Berg

Kantoor Diest
K. Albertstraat 74-76, 3290 Diest

Kantoor Wervik
Sint-Maartensplein 7, 8940 Wervik

www.advocaten-leuven.be
016 30 14 40 • info@advocaten-leuven.be

Met dank aan mevrouw Christina Van Thielen, de taalwijzer van het kantoor, voor het nalezen van de tekst.

versie mei 2018