HET GROTE

HANDBOEK

1ste editie 2018

GDPR IN DE PRAKTIJK

DE NIEUWE EUROPESE PRIVACYWETGEVING

Auteur: Viktor D'Huys, Group Joos

Co-auteur: Peter Witsenburg, Belgium Cloud & Cloud Makelaar

Inhoudstabel

Woord vooraf

"Money makes the world go round is verleden tijd, data make the world go round" Het is een uitspraak van een journalist die ik een tijdje terug las. En daar valt wel wat voor te zeggen. Data hebben een steeds grotere invloed op ons leven. Ze zijn enerzijds de voornaamste grondstof van de motor van de nieuwe digitale economie en anderzijds sturen ze via nieuwe technologieën ook steeds meer ons leven.

En dat is voor alle duidelijkheid een goede zaak. Slimme apparaten en toepassingen verbeteren ons persoonlijk leven én het samenleven met anderen. Van de apps op onze smart-phone tot nieuwe technologieën in smart cities, data helpen ons verder. Of het nu gaat over vlotte mobiliteit, betere luchtkwaliteit of gezondheidszorg op maat, de toepassingen zijn eindeloos.

Door dit geloof in hun kracht, zijn persoonsgegevens het nieuwe Eldorado geworden. De overtuiging dat ze morgen het antwoord bieden op onze problemen van vandaag, maakt dat ze enorm gegeerd zijn door ontwikkelaars. Steeds meer van wat we doen, wordt geregistreerd. De afgelopen jaren is er een gigantische toename van de digitalisering, opslag, verwerking, verspreiding en uitwisseling van massa's persoonsgegevens.

Dat brengt natuurlijk onvermijdelijk ook risico's voor de privacy van burgers met zich mee. Privacybescherming is vandaag een grotere uitdaging dan ooit tevoren. Het stelt ons voor een fundamenteel vraagstuk: hoe garanderen we enerzijds dat burgers de controle hebben over hun persoonlijke gegevens en zorgen we er anderzijds voor dat de digitale ondernemer en economie verder kan bloeien?

Met haar General Data Protection Regulation, heeft Europa hier een antwoord op geboden. Door in te zien dat de belangen van ontwikkelaars en burgers niet tegengesteld zijn maar voor een groot deel samenvallen. Burgers zijn bezorgd om hun privacy maar zijn ook op zoek naar nieuwe, vaak gepersonaliseerde toepassingen die hun levens verbeteren. Bedrijven zijn op zoek naar data om hun producten te ontwikkelen maar beseffen ook steeds meer dat klanten privacygevoelig zijn.

De oplossing waar voor gekozen is, is dan ook duidelijk: een betere bescherming en waardering van persoonsgegevens en dat in een eengemaakte Europese digitale markt. Dat hebben we gedaan met de harmonisering van de 28 verschillende praktijken in de Europese Unie.

Bedrijven moeten zich daardoor enkel nog aanpassen aan één wetgeving. Dat zorgt voor een vlottere uitwisseling van persoonsgegevens en geeft een boost aan vernieuwende en digitale toepassingen voor alle inwoners in Europa.

Tegelijkertijd zijn dataverwerkers verplicht om verantwoord om te springen met de persoonlijke gegevens van hun bestaande of nieuwe klanten. Het is daarbij aan de gegevensbeschermingsautoriteit om toe te zien op het naleven van de privacybescherming. Dit door bedrijven te begeleiden en te coachen om compliant te zijn met de nieuwe wetgeving. Sancties zijn daarbij een laatste stok achter de deur en nooit een doel op zich.

Dit alles zorgt voor een betere waardering van onze persoonsgegevens. De bedoeling van de Europese digitale strategie is immers dat bedrijven zo efficiënt mogelijk omspringen met onze kostbare persoonsgegevens. Het is de motor achter de bloeiende digitale markt waarin elke dag de limieten van de technologische vooruitgang worden verlegd. Om haar volle potentieel te ontdekken, is het van belang dat elk bedrijf zijn gegevensverwerking analyseert en optimaliseert.

De nieuwe wetgeving vervult zo haar dubbele doelstelling. Ze zorgt voor aangepaste grendels die ook in digitale tijden het grondrecht op privacy beschermen. Tegelijk laat het bedrijven in de digitale markt toe zich ten volle te ontplooien. Eén cruciale speler mogen we in dit alles niet vergeten: de organisaties die zich inzetten om burgers en bedrijven te informeren over deze nieuwe wetgeving. Met dit boek doen Group Joos en de Cloud Makelaar net dat. Daarvoor ben ik hen als staatssecretaris van privacy enorm dankbaar.

Veel leesplezier!

Philippe De Backer

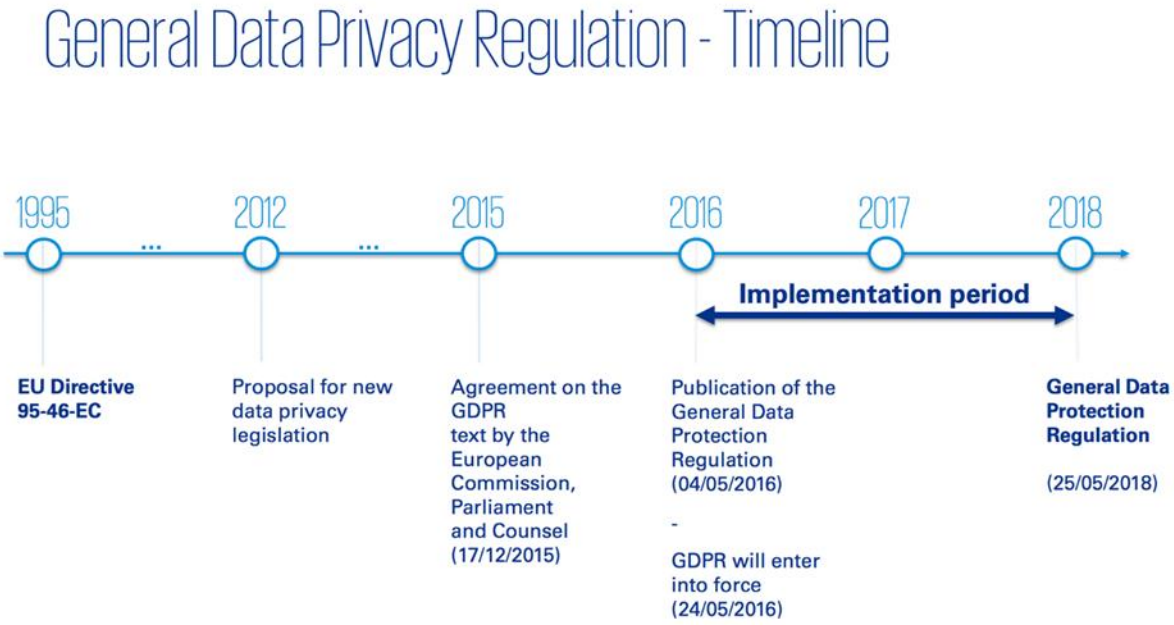
Belgisch staatssecretaris voor privacy, bestrijding van sociale fraude en de Noordzee.

GDPR: Nieuwe regels, nieuwe uitdagingen

Sinds 25 mei 2018 is de General Data Protection Regulation (GDPR) of Algemene Verordening Gegevensbescherming (AVG) van kracht. De GDPR, officieel Verordening (EU) 2016/679 van 27 april 2016, is een EU-verordening van 88 pagina's met 99 artikelen en 173 'Overwegingen'. Ze is van toepassing op elke persoon of organisatie die persoonsgegevens verzamelt of verwerkt in de EU of buiten de EU maar over personen die in de 28 lidstaten van de Europese Unie wonen of niet-Europeanen die zich in de EU bevinden. Ze is bij uitbreiding ook van toepassing voor de niet-EU-landen die tot de Europese Economische Ruimte (EER) behoren (Liechtenstein, Noorwegen en IJsland).

Met de GDPR probeert de EU een nieuw evenwicht te vinden tussen de privacy van haar burgers en de verzameling van persoonsgegevens door bedrijven. Iedereen die persoonsgegevens verzamelt, gebruikt of in opdracht van iemand anders verwerkt, moet de nieuwe regels kennen en navolgen.

Wat is er nieuw aan de GDPR en, nog belangrijker, wat betekent dit voor je bedrijf of organisatie? Want privacywetgeving is natuurlijk niet nieuw. Al sinds de goedkeuring van de Universele Verklaring van de Rechten van de Mens in 1948 bestaat er een spanningsveld tussen het recht op privacy, de vrije meningsuiting en het vrij verkeer van goederen en diensten.



Sinds de komst van het internet en big data is het zoeken naar een nieuw evenwicht. Daarbij komt de GDPR om de hoek kijken.

Met die nieuwe set regels wil de EU immers de bestaande wetgeving uniform maken voor de hele Europese Economische Ruimte (EER). Daarnaast worden de regels ook een pak strenger, en dat heeft grote gevolgen, zeker voor bedrijven die op grote schaal of als kernactiviteit persoonsgegevens verzamelen en gebruiken.

In de eerste plaats moeten de persoonsgegevens die je bedrijf bewaart, grondig beveiligd worden. Voorbeelden daarvan zijn het versleutelen van data op de website, het opslaan van data op een fysiek goed beveiligde plaats en duidelijkheid over wie binnen jouw bedrijf recht heeft op toegang tot de gegevens.

Verder moet er transparant gecommuniceerd worden over welke data je bijhoudt, wat ermee gedaan wordt en met welk doel. Bezoekers van je website moeten bijvoorbeeld hun akkoord geven om hun gegevens te gebruiken voor een vooraf meegedeeld doel. Ze moeten op de hoogte zijn welke data je bijhoudt en wat je daarmee doet. Daarbovenop moet iedereen zijn eigen data kunnen raadplegen, wijzigen en eventueel laten verwijderen. Het behoeft weinig uitleg dat aan dergelijke verplichtingen voldoen een titanenwerk is.

Ten slotte moet je in geval van een datalek een noodplan klaar hebben. In sommige gevallen moet je dat lek ook nog eens melden aan de bevoegde instanties en de getroffen personen. Daar komt nog bij dat alle regels ook gelden voor alle bedrijven die betrokken zijn in het proces, ook onderaannemers.

1. Definities

1.1 Wat zijn persoonsgegevens?

We kunnen niet praten over GDPR zonder het over de definitie van persoonsgegevens[1] te hebben. Persoonsgegevens kun je omschrijven als 'alle informatie die in verband staat met geïdentificeerde of identificeerbare natuurlijke personen'. Zoals in alle definities is daarbij ieder woord belangrijk. We bekijken hieronder elke term uit de definitie.

- Natuurlijke personen:
  Het gaat om gegevens van levende individuele personen en niet van rechtspersonen. Gegevens van firma's die je klant of leverancier zijn, vallen hier dus niet onder, maar bijvoorbeeld de gegevens van je contactpersonen dan weer wel.
- Geïdentificeerde personen:
  Je kan een persoon identificeren aan de hand van naam, voornaam, adres en geboortedatum. Hoe meer gegevens je hebt en hoe kleiner de verzameling personen, hoe gemakkelijker het is om de informatie tot één persoon terug te voeren.
- Identificeerbare personen:
  Sommige gegevens zijn op zich niet aan een persoon te koppelen, maar bevatten een sleutel waarmee je ze met andere gegevens kan combineren. Als dat toch tot een identificatie kan leiden, gaat het ook om persoonsgegevens. De GDPR zegt expliciet dat dit zo blijft zolang de combinatie gemaakt kan worden met redelijke inspanningen.
- Alle informatie:
  Hiermee wordt duidelijk aangegeven dat het niet enkel gaat over digitale informatie in gegevensbestanden, maar evengoed over verzamelde gegevens op papier, beeldmateriaal, klankopnamen… Sommige van de vroegere wetgevende initiatieven beperkten zich tot de digitale informatie, maar voor de GDPR is dat expliciet niet het geval.

- Informatie die in verband staat met een persoon:
  Ook informatie die op zichzelf niets over een persoon zegt, kan een persoonsgegeven worden doordat ze aan een persoon gekoppeld wordt. Een goed voorbeeld zijn locatiegegevens (de plaats waar iemand zich op een bepaald ogenblik bevindt).

[1] Artikel 4.1 en 4.6 : Overweging 15, 26-27 en 30-31

Het gaat dus om een zeer breed gamma aan gegevens, gaande van je naam, adres en geboortedatum via je burgerlijke staat en de namen van je partner en je kinderen tot je medisch dossier bij je huisarts of een uittreksel uit het strafregister. Informatie zoals je diploma's, je talenkennis en je werkervaring stel je vaak bewust beschikbaar. Je persoonlijke belevenissen deel je via de sociale media vermoedelijk enkel met familie en vrienden en scherm je juist af van de buitenwereld. Maar heb je al gedacht aan de lijst van alle artikelen die je het laatste jaar in je favoriete supermarkt gekocht hebt of een overzicht van alle informatie waarnaar je op het internet op zoek bent geweest? Het gaat zelfs om de exacte plaats waar je gsm op een bepaald moment was (en dus wellicht ook jijzelf).

Tip:

Om de omvang te overzien van de informatie waarop de GDPR van toepassing is, kun je alvast eens een eerste inventaris maken van de persoonsgegevens waar je zelf in je werkomgeving mee te maken hebt. Je kan ook de gegevens verzamelen waarvan je weet of vermoedt dat ze door je werkgever of door zakelijke contacten in andere firma's over jou worden bijgehouden. Lees nog niet verder en doe eerst de oefening.

Heb je je lijstje gemaakt? Heb je aan de volgende zaken gedacht?

- Een schuif vol naamkaartjes, een spreadsheet met contactgegevens.
- Het privételefoonnummer van collega's of het directe nummer van een consultant dat in vertrouwen doorgegeven is voor een noodgeval.
- Foto's van het laatste personeelsfeest.
- Je cv.
- De verslagen van evaluatie- of functioneringsgesprekken.
- Overzichten van gewerkte dagen, afwezigheden en ziektedagen.
- Camerabeelden bij de toegangen tot de bedrijfsgebouwen of op de werkvloer.
- Logs die bijgehouden worden op de ICT-afdeling: het tijdstip waarop je ingelogd bent op het netwerk of op bepaalde applicaties, de websites die je bezoekt.
- Je mailverkeer (enerzijds de inhoud maar anderzijds ook het aantal mails, de bestemmelingen…).
- Vragenlijstjes die je invult om van een leverancier informatie te ontvangen, een White paper te downloaden of op een nieuwsbrief in te tekenen (je interessedomeinen, je hobby's, je functie in je bedrijf, je jaren ervaring…).

Dit overzicht is nog lang niet volledig, maar het is duidelijk waarom er wetgeving nodig is die verzekert dat iedereen die persoonsgegevens gebruikt, er zorgvuldig mee omspringt en zich aan een aantal regels houdt. Anderzijds is het ook onvermijdelijk en zelfs noodzakelijk dat persoonsgegevens gebruikt kunnen worden, niet alleen in de privésfeer of door de overheid, maar ook door de bedrijfswereld.

De GDPR wil net zorgen voor een goed evenwicht tussen het recht op privacy van de individuen en de mogelijkheid voor bedrijven om de rijkdom aan informatie die beschikbaar is, te kunnen gebruiken, ook buiten de grenzen van een land.

In deze publicatie zal het duidelijk worden dat bij de GDPR alles draait om de balans tussen deze beide invalshoeken. Welke informatie wordt gebruikt en met welk doel, is cruciaal voor de verplichtingen waaraan men moet voldoen.

Het volgende hoofdstuk gaat dieper in op de gradaties in gevoeligheid van de persoonsgegevens en op wat de wet 'speciale categorieën' noemt. Daarna bekijken we wat men precies bedoelt met gegevensverwerking en welke rollen en verantwoordelijkheden daarbij gedefinieerd zijn.

1.2 Speciale categorieën van persoonsgegevens

Bij de GDPR draait alles rond de balans tussen je eigen bedoelingen met het verzamelen en gebruiken van persoonsgegevens en het recht van ieder individu op bescherming van zijn of haar persoonlijke levenssfeer. De aard en de hoeveelheid van de verwerkte gegevens moeten daarom altijd in proportie zijn tot het doel.

Binnen het geheel van alle persoonsgegevens zijn er grote verschillen. Sommige gegevens zijn publiek gekend of zijn zo ruim verspreid en gemakkelijk te vinden dat het bekendraken ervan nauwelijks een probleem oplevert en niet echt als een schending van de privacy kan worden beschouwd. Andere zijn zo vertrouwelijk dat de GDPR ze onderbrengt in 'special categories[2]', waarvoor extra regels gelden. Het is dus belangrijk vanaf het eerste ogenblik te beseffen dat te verwerken persoonsgegevens tot een speciale categorie behoren.

De GDPR somt de speciale categorieën daarom expliciet op:

- Informatie over ras of etnische herkomst;
- Gegevens over iemands godsdienstige of filosofische overtuiging;
- Info over politieke opvattingen van een persoon of over zijn lidmaatschap van een vakbond;
- Gegevens over het seksueel leven of de seksuele geaardheid;
- Medische informatie;
- Biometrische identificatiegegevens en DNA;
- Informatie over wetsovertredingen of strafrechtelijke veroordelingen.

De Belgische Gegevensbeschermingsautoriteit (GBA) geeft bijgaande voorbeeldlijst.

[2] Artikel 4.13-15; Artikel 9-10 : Overweging 34-35 en 51-56

Personal Data Categories (Privacy Commission)	Personal Data Category?
A. Identificatiegegeven B. Financiële bijzonderheden C. Persoonlijke kenmerken D. Fysieke kenmerken E. Leefgewoonten F. Psychische gegevens (informatie over karakter en persoonlijkheid) G. Samenstelling van het gezin H. Vrijetijdsbesteding en interesses I. Lidmaatschappen K. Consumptiegewoonten L. Woningkenmerken N. Opleiding en vorming O. Beroep P. Rijksregisternummer / Identificatienummer van de sociale zekerheid V. Beeldopnamen W. Geluidsopnamen	"Regular" Personal Data
J. Gerechtelijke gegevens M. Gegevens betreffende de gezondheid Q. Raciale of etnische gegevens R. Gegevens over het seksuele leven S. Politieke opvattingen T. Lidmaatschap vakbond U. Filosofische of religieuze overtuigingen	Special Category

Als algemene regel geldt dat je dergelijke informatie niet mag verwerken. Indien dit toch nodig is, moet je de doelstelling en de wettelijke grondslag hiervoor duidelijk vastleggen. Daar zijn specifieke regels voor. In de verschillende stadia van het verwerkingsproces gelden dan eveneens strengere normen: bij de informatiebeveiliging, bij het transfereren van dergelijke gegevens buiten de Europese Economische Ruimte (EER) en zeker bij het afhandelen van een eventueel datalek. Daarop zullen we in deze publicatie nog meermaals terugkomen.

Ook buiten deze speciale categorieën kan je nog altijd een onderscheid maken tussen gegevens met een beperkt risico op schending van de privacy en meer gevoelige informatie. Financiële informatie is bijvoorbeeld gevoeliger dan een adres. Gegevens over kinderen moet je altijd extra zorgvuldig behandelen.

Als je persoonsgegevens verzamelt en gebruikt, moet je dus altijd de afweging maken of je deze gegevens echt nodig hebt voor het beoogde doel en hoe groot het risico is dat er een inbreuk op iemands privacy zou kunnen ontstaan. Hoe groter het aantal personen en hoe meer gegevens je over hen verzamelt, hoe hoger het risico. Dit is in essentie wat bedoeld wordt met het maken van een dataprivacy impact analyse (DPIA). Naargelang de omstandigheden kan daar een heel project voor nodig zijn of volstaat een simpele afweging (die wel geregistreerd moet worden). Dat werken we later nog verder uit.

Er zijn ook een aantal stappen mogelijk om de te verwerken persoonsgegevens minder gevoelig te maken. De beste oplossing is te werken met anonieme gegevens.

Als de data correct geanonimiseerd zijn (dat betekent dat ze niet meer kunnen teruggevoerd worden op individuen), zijn het geen persoonsgegevens meer en is de GDPR niet meer van toepassing. Deze werkwijze wordt waar mogelijk toegepast op gegevens voor wetenschappelijk onderzoek en is eveneens aangewezen voor grootschalige gegevensverwerking voor gebruik in marketing. Eén van de gebruikte methodes is het samenvoegen van gegevens in groepen.

Een belangrijke voorwaarde is dan dat het over een voldoende groot aantal gegevens gaat, zodat de groepen steeds meer dan een paar individuen bevatten (50 wordt weleens als een minimum gesteld). Je moet je ervan bewust zijn dat hoe meer verschillende gegevens verzameld worden, hoe groter de kans is dat je door een combinatie ervan iemand kan identificeren.

Een andere veel gebruikte methode is pseudonimisatie[3]. Bij die werkwijze worden in een dataset alle elementen verwijderd die een persoon identificeren en vervangen door een nietszeggende sleutel. Het sleutelbestand wordt afzonderlijk bewaard.

[3] Artikel 4.5; Artikel 25 : Overweging 78

Dergelijke gegevens zijn nog steeds persoonsgegevens, want ze hebben betrekking op een identificeerbare persoon. Wel is het zo dat het risico op impact voor een betrokkene aanzienlijk kleiner is. Pseudonimiseren geldt dus als een goede beveiligingsmaatregel, bijvoorbeeld voor gevoelige gegevens die moeten overgedragen worden.

De definities van persoonsgegevens en welke persoonsgegevens gevoelig zijn of tot speciale categorieën behoren, zijn in de GDPR niet wezenlijk anders dan in de oudere wetgeving omtrent privacy.

Bij alle overwegingen over de betekenis van de GDPR moeten we hiervan uiteraard vertrekken. In het volgende hoofdstuk gaan we dieper in op het verwerken van persoonsgegevens en op de verschillende rollen die de wet onderscheidt. Daar zijn er wel essentiële verschillen tussen de GDPR en de vroegere regelgeving.

1.3 Gegevensverwerking en de verschillende rollen

Om een inschatting te maken van wat de GDPR voor je eigen bedrijf of voor jouw job betekent, moet je niet alleen weten welke gegevens persoonsgegevens zijn.

Je moet ook goed begrijpen wat de wet precies bedoelt met gegevensverwerking[4]. Inzicht hebben in de verschillende mogelijke rollen bij het verwerken van persoonsgegevens is ook belangrijk. Welke rol je speelt, bepaalt immers in grote mate je verantwoordelijkheden en je verplichtingen.

Gegevensverwerking

Gegevensverwerking moet je heel breed zien. We denken spontaan aan het verzamelen van contactgegevens, interesses, aankoopgedrag, websitebezoeken, enz. Die informatie gebruikt men dan voor marketing- of verkoopcampagnes.

Het gaat echter breder dan dat. Eigenlijk is om het even welke activiteit die te maken heeft met data van personen een vorm van gegevensverwerking waarop de GDPR van toepassing is.

Gegevens bekijken of raadplegen, gegevens bewaren, gegevens wissen of verwijderen, gegevens transporteren… Het zijn allemaal voorbeelden van wat de wet bedoelt met gegevensverwerking.

Als straks iedereen een inventaris maakt van gegevensverwerkingen die hij zelf uitvoert of toevertrouwt aan derden, is het belangrijk dit ruim genoeg te zien.

[4] Artikel 2.1-2; Artikel 4.2

Dat een firma die personeelsbeheer voor derden doet, persoonsgegevens verwerkt, spreekt voor zich. Maar ook de leverancier die in opdracht van je firma oud papier komt ophalen, doet aan gegevensverwerking als het gaat om individueel gepersonaliseerde documenten.

Het gebruik van persoonsgegevens door privépersonen in de huiselijke sfeer[5] valt echter niet onder de GDPR. Het werk van het gerecht en van de ordediensten evenmin, omdat dit door andere wetgeving geregeld wordt.

De rollen

Bij het verwerken van gegevens onderscheidt de privacywetgeving verschillende rollen. De belangrijkste zijn de 'Verantwoordelijke' en de 'Verwerker' (in Nederland zegt men 'Bewerker'). Vaak worden hiervoor ook de Engelse termen 'Data Controller' en 'Data Processor' gebruikt.

De **Verantwoordelijke[6]** is degene die het initiatief neemt om persoonsgegevens te (laten) verzamelen en bij te houden, met de bedoeling die op een of andere manier te verwerken.

De Verantwoordelijke moet het specifieke doel vastleggen van de gegevensverwerking en aantonen dat hij daarvoor een gewettigde grond heeft. Hij moet vooraf overwegen welke persoonsgegevens hiervoor nodig zijn.

Essentieel voor de wetgeving is dat niet meer gegevens worden verzameld en verwerkt dan strikt noodzakelijk is om het doel te bereiken. Gegevens niet verwerken is immers de best mogelijke bescherming van de privacy.

De Verantwoordelijke garandeert ook de veiligheid van de verzamelde gegevens. Hij verzekert hun beschikbaarheid en zorgt dat de integriteit te allen tijde bewaard wordt (dit wil zeggen dat ze niet onterecht gewijzigd of gewist worden) en dat er geen inbreuken gepleegd worden op de vertrouwelijkheid. Een belangrijk onderdeel daarvan is dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor ze verzameld zijn.

[5] Artikel 2.2c : Overweging 18
[6] Artikel 4.7

De rol van de **Verwerker**[7] daarentegen is dat hij persoonsgegevens van een Verantwoordelijke ter beschikking krijgt en deze gebruikt volgens de instructies van de Verantwoordelijke, in functie van diens doelstelling. Deze rol kan uiteraard ook door de Verantwoordelijke zelf opgenomen worden. Als deze echter een beroep doet op een derde partij, heeft die laatste enkel de rol van Verwerker.

Dit is een fundamenteel onderscheid, dat de basis vormt voor de wettelijke verplichtingen. Een belangrijke vaststelling is alvast dat anders dan in de vroegere privacywetgeving de GDPR ook expliciet verplichtingen oplegt aan de Verwerker.

Het is wel goed te beseffen dat de taakverdelingen soms niet zo zuiver af te lijnen zijn. Zo is het bijvoorbeeld perfect mogelijk dat de persoonsgegevens eigenlijk verzameld worden door een Verwerker. Een Verantwoordelijke kan immers aan een Verwerker de taak geven persoonsgegevens te verzamelen, te verrijken en te analyseren als deel van de opdracht. Deze taken zijn alle voorbeelden van wat de wet bedoelt met 'verwerking van persoonsgegevens'.

Het is niet omdat je de gegevens verzamelt, dat je automatisch de Verantwoordelijke bent, maar omgekeerd blijf je als opdrachtgever wel verantwoordelijk, ook al besteed je het verzamelen van de gegevens uit aan een Verwerker.

[7] Artikel 4.8

In de toekomst zal een contract duidelijk moeten aangeven wat de rollen van de opdrachtgever en de opdrachtnemer zijn in de gegevensverwerking. Een belangrijke tip is om hieraan steeds de nodige aandacht te besteden. De nieuwe wet gaat er trouwens van uit dat gegevensverwerking altijd omkaderd wordt door een verwerkersovereenkomst, waarin de wederzijdse verplichtingen ten aanzien van dataprivacy duidelijk zijn vastgelegd. Tegelijk moet je beseffen dat je verantwoordelijkheden samenhangen met de rol die je feitelijk speelt, ongeacht wat in een contract is opgenomen. Dit wil zeggen dat je er als Verwerker op moet letten om geen verantwoordelijkheden op te nemen die niet bij je rol horen. De belangrijkste en meest evidente beperking is dat je de gegevens die de Verantwoordelijke je toevertrouwt nooit voor een ander doel mag gebruiken dan in je opdracht is vastgelegd.

Ten slotte bepaalt de wet ook een duidelijke derde rol, die van de **Betrokkene**[8] (of in het Engels 'Data Subject'). De betrokkene is de individuele persoon op wie specifieke persoonsgegevens betrekking hebben. Het is in eerste instantie de Betrokkene die door de wet beschermd wordt.

De GDPR kent de Betrokkene expliciet een aantal rechten toe over zijn persoonsgegevens. Dit is een fundament van de nieuwe verordening. Om te beginnen vereist de GDPR-openheid over gegevensverwerking tegenover de betrokkenen. Daarnaast hebben zij ook recht op wat meestal samengevat wordt als 'fair use' van de data.

Hieronder valt zowel het legaal verwerven en verwerken van gegevens, als de zorg om ze accuraat te houden, ze voldoende te beveiligen en ze enkel te gebruiken voor het gestelde doel.

De Betrokkene heeft het recht om over al deze aspecten geïnformeerd te worden. Last but not least kan de Betrokkene in grote mate beschikken over zijn individuele data. Hij kan ze opvragen, ze laten corrigeren, ze laten wissen of de verwerking ervan laten stopzetten.

De rechten en plichten die met elke rol samenhangen komen verder in deze publicatie nog uitvoerig aan bod.

[8] Artikel 12

1.4 De Data Protection Officer (DPO)

Er is een grote kans dat de Data Protection Officer[9] (DPO), of in het Nederlands de Functionaris voor Gegevensbescherming, een belangrijke plaats zal innemen in je GDPR-traject. In dit hoofdstuk bekijken we welke bedrijven een DPO moeten hebben en wat de rol van die persoon is.

Het is niet zo dat de GDPR elke verantwoordelijke verplicht een DPO aan te stellen. Tijdens de voorbereidende besprekingen leek het er lange tijd op dat de verplichting zou gelden voor alle firma's met minstens 250 werknemers. Deze bepaling is echter niet overeind gebleven. De verplichting is nu eerder gebaseerd op de aard van de onderneming. Als er bij de activiteiten van een organisatie een reëel risico op ernstige inbreuken tegen de privacy bestaat, moet er een DPO zijn die zorgt dat je in regel bent met de wetgeving.

Dat risico hangt af van de hoeveelheid verwerkte data, de aard van de data of de frequentie van de verwerkingen. Een aantal organisaties moeten sowieso een DPO aan boord hebben: alle overheidsorganisaties, alle bedrijven die als hoofdbezigheid speciale categorieën van persoonsgegevens verwerken en alle bedrijven of organisaties die als hoofdbezigheid systematisch op grote schaal persoonsgegevens verzamelen en verwerken.

Ook als het niet wettelijk verplicht is, is het aan te raden iemand expliciet de rol van DPO te geven. Zo heb je meteen een voortrekker voor het voorbereidingstraject. De DPO zal ervoor zorgen dat in je bedrijf een cultuur van gegevensbescherming heerst, dat het item dataprivacy op de agenda komt en dat je firma tijdig klaar is voor de GDPR.

De DPO zal voor zijn taak de tijd moeten krijgen om de wetgeving te bestuderen en zich in de materie in te werken, maar die kennis kan daarna wel doorstromen naar de rest van de organisatie. Het is ook logisch dat de DPO een leidende rol speelt in het GDPR-project.

[9] Artikel 37-39 : Overweging 97

Voorwaarden voor de Data Protection Officer

Een bedrijf dat een DPO moet aanstellen, moet rekening houden met een aantal voorschriften. Je moet de naam en contactgegevens van de DPO aan de gegevensbeschermingsautoriteit bekendmaken. In België is de GBA de vroegere Privacy commissie, in Nederland de Autoriteit Persoonsgegevens (AP).

De DPO moet niet alleen deskundig zijn inzake privacywetgeving, maar ook een grondige kennis hebben van zijn eigen bedrijf, de werking ervan en de markt waarin het opereert. Hij moet ook voldoende gezag hebben en voldoende middelen krijgen om zijn taak te vervullen.

Er wordt verwacht dat hij aan het seniormanagement rapporteert en dus voldoende onafhankelijk is. Er mag ook geen belangenvermenging optreden.

Daarom zal bijvoorbeeld een ICT-verantwoordelijke meestal niet tegelijkertijd DPO mogen zijn, omdat hij anders de beveiligingsmaatregelen zou moeten controleren die zijn eigen team opzet. Hoe een en ander concreet wordt ingevuld, hangt uiteraard af van de omvang van de organisatie.

In een klein bedrijf zal de DPO-rol geen fulltime opdracht zijn, maar met andere taken gecombineerd worden. De DPO-functie kan ook perfect door een externe persoon worden uitgeoefend.

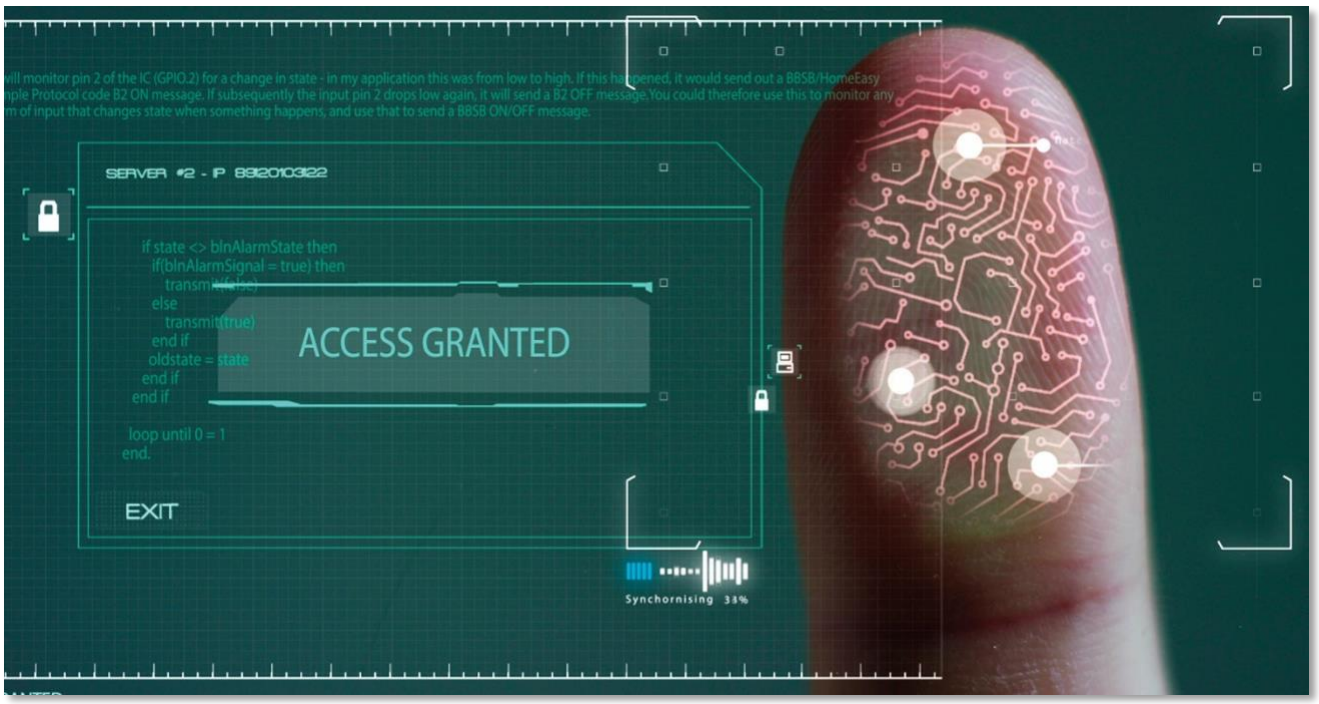
De GDPR schrijft niet voor welk diploma of welke certificaten een DPO moet hebben en legt ook niet vast of juridische dan wel organisatorische of technische voorkennis en ervaring primeren. Zelfs in een kleine organisatie is uiteraard een minimum aan kennis nodig. Het loont zeker om buiten de kennisopbouw, die kan gebeuren op allerlei fora, ook te investeren in enkele dagen specifieke opleiding.

Een DPO is een voordeel

Een DPO hebben is dus zeker een groot voordeel, ook al is het in je specifieke situatie niet wettelijk verplicht. De DPO kan een rol spelen in elk van de voorbereidende stappen om klaar te zijn voor de GDPR.

Het is trouwens zo dat er bij verschillende andere procedures rond persoonsgegevens nog belangrijke taken weggelegd zijn voor de DPO. Hij wordt ingeschakeld bij het opzetten van elke nieuwe verwerking van persoonsgegevens en geeft advies over risico's en noodzakelijke beschermingsmaatregelen.

Hij is betrokken bij de opvolging van incidenten of echte datalekken en is daarvoor het eerste aanspreekpunt, zowel voor klanten en betrokkenen als voor de Belgische gegevensbeschermingsautoriteit. Ten slotte verzekert de DPO als een primaire taak de rechten van de betrokkenen. Hij is hun rechtstreeks aanspreekpunt. De DPO zullen we dus in andere hoofdstukken van deze publicatie nog regelmatig tegenkomen.



2. Basisbeginselen van de GDPR

In dit hoofdstuk leiden we uit de basisbeginselen van de GDPR[10] af welke verplichtingen je hebt als verantwoordelijke voor de verwerking van persoonsgegevens. We voegen er meteen 6 stappen aan toe die je moet nemen om in regel te zijn met de GDPR.

Eerlijk gebruik van persoonsgegevens

De GDPR wil een regelgevend kader scheppen om het gebruik van persoonlijke informatie door bedrijven en organisaties mogelijk te maken en tegelijk de privacy van de betrokkenen zo goed mogelijk te beschermen.

De basisprincipes voor een gerechtvaardigd gebruik van persoonsgegevens zijn:

- Open zijn over de data die je bijhoudt en de verwerkingen die je doet;
- De data wettig en eerlijk gebruiken;
- De rechten van de betrokkenen vrijwaren;
- Vertrouwelijkheid en integriteit van de gegevens respecteren;
- Aansprakelijk zijn als verantwoordelijke.

Deze beginselen zijn al heel lang in de privacywetgeving aanwezig en zijn in de loop van de tijd stelselmatig duidelijker omlijnd.

De belangrijkste verplichtingen die de GDPR oplegt aan een verantwoordelijke voor de gegevensverwerking, vloeien rechtstreeks uit deze beginselen voort.

- Openheid bereik je door duidelijk kenbaar te maken welke persoonsgegevens je bijhoudt, welke verwerking je doet en welke doelstelling je ermee nastreeft. De informatie hierover moet gemakkelijk terug te vinden zijn en in klare, eenvoudige taal opgesteld worden, zodat iedereen het kan begrijpen.
- Eerlijk gebruik van persoonsgegevens houdt in dat je de gegevens op een legale manier verwerft, dat je ze enkel gebruikt voor het vooropgestelde doel en dat je niet meer data verzamelt en ze niet langer bijhoudt dan nodig is voor dat doel.
- Elke betrokkene heeft recht op informatie over de verwerking van zijn data. Hij kan inzage vragen in de concrete gegevens en kan deze laten verbeteren, aanvullen of verwijderen. Hij kan de verwerking in bepaalde omstandigheden laten stopzetten. Het zal een hele klus zijn om al deze rechten te respecteren.

[10] Artikel 5 : Overweging 39

- Respect voor de data betekent dat je er alles aan doet om ze kwalitatief zo correct mogelijk in te voeren en actueel te houden en dat je ze adequaat beveiligt. Zo worden ze niet onterecht openbaar gemaakt of voor verkeerde doeleinden gebruikt.
- De verantwoordelijke kan aantonen dat hij aan alle verplichtingen van de regelgeving voldoet en is aansprakelijk bij tekortkomingen.

Wie maatschappelijk verantwoord ondernemen hoog in het vaandel draagt, schaart zich logischerwijze achter deze doelstellingen. De GDPR en de verdere toelichtingen die door de nationale gegevensbeschermingsautoriteiten, in België de GBA, de vroegere Privacy commissie, in Nederland de Autoriteit Persoonsgegevens, worden verstrekt, moeten we dan ook zien als een hulpmiddel.

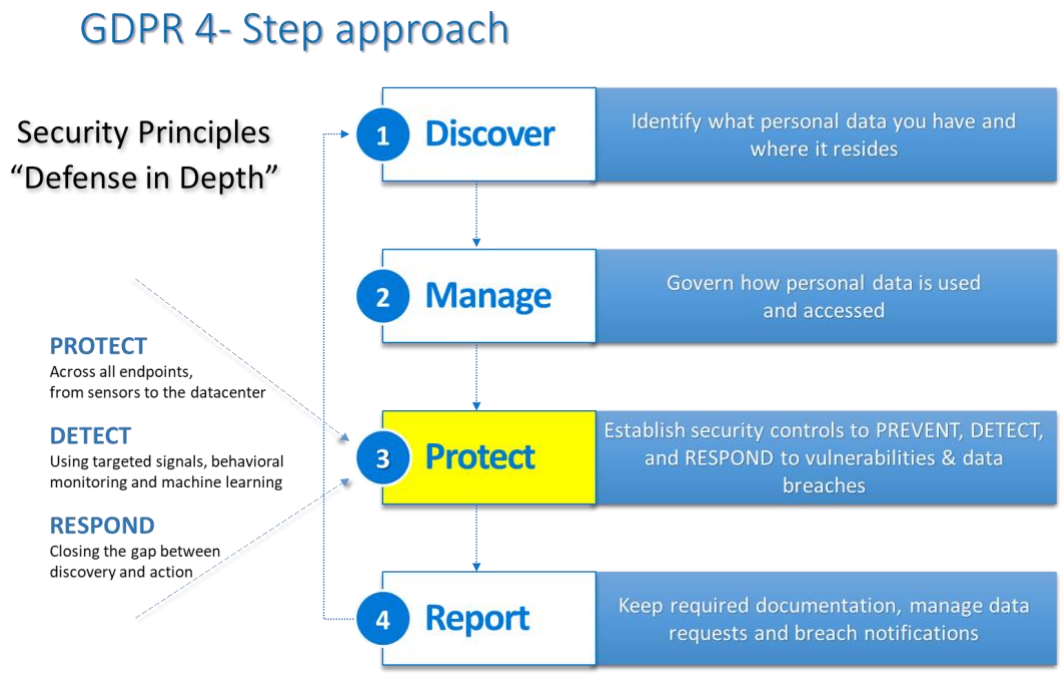
Ze bieden een houvast om een waardevol doel te bereiken zonder dat de werking of organisatie van een bedrijf onmogelijk gemaakt wordt. Het is immers niet de bedoeling dat de GDPR zou leiden tot een privacy kramp.

Voorbereidingstraject voor de GDPR

De belangrijkste stappen die een verantwoordelijke voor gegevensverwerking moet nemen om in orde te zijn met de nieuwe regelgeving sommen we hier kort al even op.

- Leg een **register** aan **van verwerkingen van persoonsgegevens**. Je moet dit register kunnen voorleggen aan de gegevensbeschermingsautoriteit (België) of Autoriteit Persoonsgegevens (Nederland) als zij erom vragen. Zie dit in de eerste plaats als een hulpmiddel voor jezelf. Je krijgt immers een beeld van alle persoonsgegevens waarvan je gebruik maakt. Het register vermeldt het type gegevens, de soort verwerking, het doel en de wettelijke grond voor de verwerking.
- Stel **een privacyverklaring** op. Op alle plaatsen waar je contactgegevens en andere informatie over personen verzamelt, moet deze gemakkelijk raadpleegbaar zijn.
- Ga na of je een **adequate beveiliging** hebt voor alle verzamelde persoonsgegevens. Is je netwerk veilig? Bewaar je bestanden met persoonsgegevens versleuteld of met een veilig wachtwoord? Worden gegevens die niet meer nodig zijn, veilig verwijderd (zowel de digitale als de papieren informatie)?

- Werk de nodige instructies uit voor **wat** er moet gebeuren **als een betrokkene contact opneemt om zijn rechten uit te oefenen**, zodat je tijdig de noodzakelijke acties kunt nemen. Bij wie komt de vraag terecht? Wie doet wat?
- Stel een duidelijke **procedure** op met alle te nemen stappen **als er een datalek ontstaat** en er gevaar is dat de privacy van betrokkenen geschonden wordt. Zijn alle werknemers op de hoogte van deze procedure?
- Als je **derde partijen** inschakelt bij de verwerking van persoonsgegevens, zorg dan voor een **contractuele overeenkomst** die duidelijk omschrijft wat de onderaannemer precies moet doen en welke zijn verplichtingen en verantwoordelijkheden zijn onder de GDPR.



Elk van deze actiepunten werken we in de volgende hoofdstukken heel concreet uit. We willen ons immers niet beperken tot wat algemene beschouwingen, maar ook praktisch bruikbare tips geven.

3. Register van verwerkingen van persoonsgegevens

3.1 Inventaris persoonsgegevens en registerplicht

Het beste beginpunt voor GDPR-compliancy is een goede inventaris van de persoonsgegevens die je als firma of organisatie bijhoudt en gebruikt. Wellicht moet je die informatie ook omzetten in een formeel Register[11] van de verwerkingen van persoonsgegevens. Bepalen of dit Register in jouw geval verplicht is, kan een moeilijke zaak zijn. In dit hoofdstuk proberen we hierover duidelijkheid te brengen.

Inventaris van persoonsgegevens

Grote organisaties zetten voor het inventariseren van hun persoonsgegevens gespecialiseerde software in, maar op zich kan een eenvoudige spreadsheet met de benodigde informatie even goed volstaan.

Tip:
Aan de hand van een gesprek met je verschillende afdelingen kom je al veel te weten.

- Welke persoonsgegevens verzamelen en/of gebruiken ze (welke categorieën gegevens, van welk type personen, over welk aantal betrokkenen)?
- Hoe worden de gegevens verwerkt (wat wordt ermee gedaan) en met welk doel?
- Met welke leverancier, partner of andere derde worden de gegevens gedeeld?
- Worden de data mogelijk buiten de Europese Economische Ruimte (EER) getransporteerd?

Vervolgens moet je je de vraag stellen of de doelstelling van het gebruik van die informatie gerechtvaardigd is in vergelijking met het recht op privacy van de betrokkenen. Ten slotte ga je na welke bedreigingen er zijn voor het vrijwaren van de vertrouwelijkheid en integriteit van de gegevens en met welke maatregelen je ze beschermt.

[11] Artikel 30 : Overweging 82

Deze vragen hoort elke verantwoordelijke voor het verwerken van persoonsgegevens zich sowieso te stellen.

Het resultaat van deze oefening levert meteen het merendeel van de informatie op die je nodig hebt voor een register van de verwerkingen van persoonsgegevens, een nieuwe verplichting van de GDPR.

Register van verwerkingen van persoonsgegevens

De 'oude' privacywet kent een aangifteplicht van geautomatiseerde verwerkingen van persoonsgegevens aan de toezichthoudende autoriteit. In België was dat de Commissie voor Bescherming van de Persoonlijke Levenssfeer (CBPL), meestal kortweg de Privacy commissie genoemd. Die informatie werd in een publiek register opgenomen, dat iedereen kon raadplegen.

Het meest courante gebruik van persoonsgegevens was hiervan vrijgesteld, bijvoorbeeld personeelsbeheer, loonadministratie en boekhouding, klanten- en leveranciersbeheer, contactgegevens (zonder bijkomende informatie), ledenlijsten van verenigingen, studentenadministratie… Daardoor moesten de meeste organisaties geen aangifte doen.

Met de GDPR verandert dat en moet de verantwoordelijke voor de verwerking zelf een register bijhouden. Dat register moet digitaal zijn en moet snel en gemakkelijk kunnen worden voorgelegd bij een audit door de gegevensbeschermingsautoriteit, in België de GBA, in Nederland de AP, of in het kader van het onderzoek naar een klacht of een datalek. Het moet aantonen dat de verantwoordelijke een duidelijk overzicht heeft van de persoonsgegevens die hij verwerkt. Hij bewijst ermee dat hij heeft nagedacht over zijn recht om deze verwerkingen te doen en dat hij de informatie afdoende beveiligt.

Een ander verschil met de oude privacywet is dat de GDPR zich niet beperkt tot geautomatiseerde gegevensverwerking en geen uitzondering meer maakt voor de 'courant gebruikte persoonsgegevens'.

Voor wie geldt de registerplicht?

Voor kleine organisaties wordt tot op zekere hoogte een uitzondering gemaakt op deze registerplicht[12], maar de GDPR is hierover niet heel duidelijk.

Daarom heeft de Privacy commissie in België op 14 juni 2017 een uitgebreide aanbeveling gepubliceerd, waarvan we hier de belangrijkste punten samenvatten.

[12] Artikel 30.5 : Overweging 13

- Elke verantwoordelijke (en verwerker – maar daarover later meer), ongeacht of het een firma, een overheidsorganisatie, een vereniging of een natuurlijke persoon is, moet een register van de verwerkingen van persoonsgegevens bijhouden.

- Voor organisaties met minder dan 250 werknemers (en minder dan 50 miljoen euro omzet) wordt echter een uitzondering gemaakt. Dit standpunt strookt eigenlijk niet met de geest van de wetgeving, vermits alle maatregelen moeten voortvloeien uit de risicoanalyse. Het verwerken van persoonsgegevens in een kleine organisatie kan evenveel of zelfs meer risico inhouden. Daarom zijn er een hele reeks bijkomende gevallen waar de registerplicht toch blijft bestaan, ook voor de kmo.

- De registerplicht kan niet wegvallen als
    - Speciale categorieën van persoonsgegevens of gegevens van extra kwetsbare personen zoals kinderen verwerkt worden.
    - De verwerking risico's inhoudt voor de rechten en vrijheden van individuen en dus kan leiden tot ernstige lichamelijke, materiële of immateriële schade. De aanbeveling geeft een aantal voorbeelden: als er risico is op het schenden van vertrouwelijkheid van financiële info of gegevens die door beroepsgeheim beschermd worden, als er risico is op identiteitsdiefstal of fraude, als gegevens omtrent gezondheid, persoonlijkheid, gedrag, verplaatsingen enz. gebruikt worden om persoonlijke profielen op te stellen.
    - De betrokkene niet de mogelijkheid heeft zijn persoonlijke rechten uit te oefenen en dus geen controle heeft.
    - Een verantwoordelijke de persoonsgegevens niet incidenteel maar structureel verwerkt, waarmee bedoeld wordt dat niet toevallig of eenmalig informatie verwerkt wordt, maar 'gewoonlijk'. Als voorbeeld geeft de nota informatie over klanten, leveranciers, werknemers.

Zoals je ziet blijft het een erg moeilijke oefening en is de afbakening niet helemaal duidelijk. Elke organisatie heeft wel een of ander gegeven dat bij schending van de vertrouwelijkheid schade kan toebrengen en elke organisatie houdt sommige gegevens structureel bij. De Gegevensbeschermingsautoriteit in België of de Autoriteit Persoonsgegevens in Nederland raden dan ook aan dat elke firma en organisatie een register bijhoudt, maar dat zo'n register bij KMO's en MKB's beperkt mag blijven tot de gegevens die structureel worden verwerkt. In een kleine firma of organisatie blijft de oefening daardoor nog relatief beperkt.

3.2 Register van verwerkingen van persoonsgegevens

In dit hoofdstuk gaan we wat dieper in op de inhoud van het register van verwerkingen van persoonsgegevens[13]. Alle verantwoordelijken houden best zo'n register bij, ook al is het voor kleine organisaties strikt gezien niet altijd verplicht.

De eerste stap is een eenvoudige lijst van persoonsgegevens waarmee je bedrijf of organisatie werkt. De Belgische Gegevensbeschermingsautoriteit (GBA) licht toe welke vereisten het register verder stelt en groepeert dit rond zes eenvoudige vragen: Wie? Waarom? Wat? Waar? Tot wanneer? Hoe? Op hun site vind je een korte samenvatting, een omstandige nota en zelfs een modelregister dat je kan downloaden. We overlopen de zes vragen.

Wie?

Je register legt in de eerste plaats vast wie de verantwoordelijke is. Dat gaat dan om de correcte (contact)gegevens van je firma of organisatie en de naam en de gegevens van je Data Protection Officer. Als je die niet hebt, gaat het om de te contacteren persoon bij vragen, problemen, klachten of datalekken.

In grote organisaties is het nuttig te specificeren welke afdeling of persoon voor elke aparte set persoonsgegevens verantwoordelijk is. Deze verantwoordelijke zal immers het aanspreekpunt zijn om te helpen bij het invullen van de overige punten van het register.

Waarom?

Een heel belangrijke vraag is voor welk doel je persoonsgegevens gebruikt. Het basisprincipe van elke privacywetgeving en zeker van de GDPR is immers dat je enkel informatie verzamelt en verwerkt als dit strikt noodzakelijk is voor het gestelde doel. Om te communiceren met klanten en leveranciers heb je uiteraard contactgegevens nodig. Voor de sales- en marketingactiviteiten van je firma is het nodig namen en adressen te verzamelen. Bovendien is het wenselijk die basisgegevens te verrijken met extra informatie, zoals de geografische spreiding van klanten of de sector waarin ze actief zijn.

De Belgische GBA beklemtoont dat de doelstelling zo concreet mogelijk gemaakt moet worden en duidelijk de noodzaak aantoont om de betreffende informatie te verwerken.

Hun nota heeft een bijlage met een overzicht van doeleinden en nadere preciseringen. Deze kan je gebruiken als hulpmiddel.

[13] Artikel 30.1 : Overweging 39

Het is ook nuttig om stil te staan bij de wettelijke grond die je organisatie heeft om deze persoonsgegevens te verwerken, hoewel dit strikt gezien niet in het register hoeft opgenomen te worden. Dit gegeven zal in een aantal gevallen tot specifieke verplichtingen of te volgen procedures leiden. Deze aanduiding meteen aan het register toevoegen, maakt het later makkelijker om te controleren of je aan alle wettelijke verplichtingen voldoet.

Wat?

Vervolgens leg je voor elk doel vast van welke categorieën van personen de verwerkte persoonsgegevens afkomstig zijn, bijvoorbeeld je klanten, werknemers, bezoekers… Geef meteen ook aan over welke aantallen het ongeveer gaat, vermits dat een idee kan geven van de impact als er ooit een datalek ontstaat.

Vervolgens voeg je hieraan toe welke informatie je over deze personen bewaart en gebruikt: gaat het enkel om namen en adressen of verzamel je ook info over leeftijd, geslacht, functie, interesses…? Een bijlage bij de toelichting van de Belgische GBA geeft een lijst met mogelijke categorieën.

Het is heel belangrijk om expliciet te vermelden of bepaalde informatie onder de speciale categorieën valt (zie hoofdstuk 1.2). Daarvoor gelden immers speciale regels en beperkingen. Dit geldt eveneens voor informatie die niet tot deze speciale categorieën behoort maar toch als gevoelig beschouwd kan worden, zoals bijvoorbeeld financiële informatie of gegevens over minderjarigen.

Waar?

Voor elk geïdentificeerd doel moet het register opsommen waar de verwerkte informatie terechtkomt. Dit kunnen natuurlijke personen zijn, maar ook een overheidsinstelling of een interne of externe verwerker. Alle bestemmelingen worden met naam en toenaam vermeld.

Een belangrijke aanvulling hierbij is of de informatie uitsluitend verwerkt wordt binnen de Europese Economische Ruimte (EER). Als gegevens daarbuiten terechtkomen, moet je garanties hebben dat de persoonsgegevens eveneens adequaat beveiligd worden en de betrokkenen dezelfde rechten en bescherming genieten. Dit moet in het register aangetoond worden.

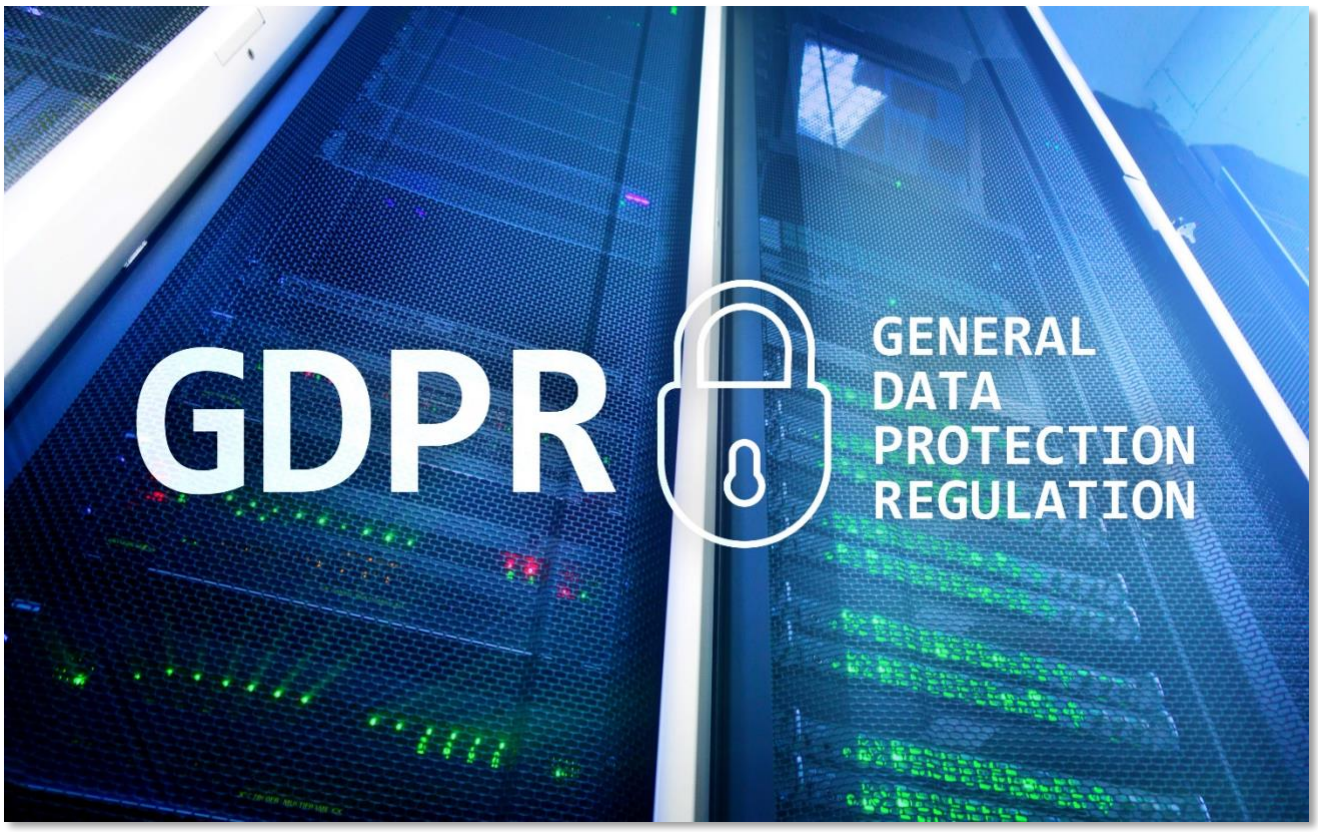
Tot wanneer?

Vermits gegevens enkel voor het beoogde doel gebruikt mogen worden, is het ook vanzelfsprekend dat je ze niet langer bijhoudt dan noodzakelijk is voor dat doel. De Belgische Privacy commissie geeft aan dat je de bewaartermijnen niet altijd in een aantal dagen, maanden of jaren moet uitdrukken. Een formulering als 'de wettelijk voorgeschreven bewaartermijn' is ook mogelijk.

Hoe beschermen we de gegevens?

Als verantwoordelijke ben je onder de GDPR aansprakelijk voor de bescherming van de verwerkte persoonsgegevens. Je moet alle noodzakelijke maatregelen nemen om te voorkomen dat hun vertrouwelijkheid of integriteit in het gedrang komt. Ze mogen niet onterecht openbaar gemaakt of doorgegeven worden aan verkeerde bestemmelingen en ze mogen niet onrechtmatig gewijzigd worden.

Indien je het register zo volledig en secuur mogelijk invult, beschik je over een goede basis om aan te tonen dat je bewust met de verwerking van persoonsgegevens omgaat en je aansprakelijkheid ernstig neemt. Dit register is tegelijk het vertrekpunt om je eigen interne procedures uit te werken en te controleren of ze correct worden toegepast. Ten slotte zal het een goede hulp zijn bij het opstellen van een privacyverklaring.



4. Rechtsgrond voor de verwerking

4.1 Rechtsgrond voor het verwerken van persoonsgegevens

Bij het opstellen van het register van verwerkingen van persoonsgegevens kan de verantwoordelijke best ook telkens de rechtsgrond[14] vastleggen, ook al is dat geen verplicht onderdeel van het register. Voor een legaal gebruik van de gegevens moet er immers een specifiek doeleinde en een aantoonbare rechtsgrond zijn voor de verwerking. Bovendien moet de verwerking de regels van subsidiariteit en proportionaliteit volgen. Ze moet met andere woorden noodzakelijk zijn en in verhouding tot het doel.

De GDPR voorziet meerdere mogelijke rechtsgronden, die niet in alle gevallen van toepassing zijn. Het is belangrijk om goed na te denken welke grond je hebt vooraleer je aan een verwerking begint. Dit proces moet gedocumenteerd worden en kan achteraf een belangrijke rol spelen bij betwistingen of klachten.

De duidelijkste en meest specifieke instructies geeft de GDPR omtrent **toestemming van de betrokkene** als rechtsgrond, maar deze behandelen we uitgebreid in het volgende hoofdstuk.

Daarnaast kunnen nog andere rechtsgronden ingeroepen worden. **De gegevens kunnen nodig zijn voor de uitvoering of de voorbereiding van een contract**. Voor de samenwerking tussen klanten en leveranciers zijn allerlei persoonsgegevens noodzakelijk. In de eerste plaats contactgegevens, maar in de B2C-wereld komen daar bijvoorbeeld betaalgegevens en financiële informatie bij. Voor zover de verwerkte informatie aantoonbaar noodzakelijk is om het contract tot stand te brengen of de overeengekomen dienstverlening uit te voeren, volstaat deze rechtsgrond als rechtvaardiging.

Een **wettelijke verplichting** kan eveneens de grondslag vormen voor het verwerken van persoonsgegevens. Het kan gaan om Europese of landelijke wetgeving die bedrijven verplicht informatie door te geven aan de overheid. Dat is het geval voor bijvoorbeeld banken, verzekeringsmaatschappijen, luchtvaartmaatschappijen, enz.

Vervolgens kan het **algemeen belang** een rechtsgrond zijn, bijvoorbeeld als de overheid organisatorische afspraken maakt met bedrijven om belastingen te administreren.

[14] Artikel 6 : Overweging 40-50

Deze rechtsgrond laat ook toe om gegevens te verzamelen voor wetenschappelijke of historische doeleinden. Taken van de publieke autoriteiten vallen eveneens onder het algemeen belang.

Verder voorziet de wet dat je **in zaken van levensbelang** (als het letterlijk over leven of dood gaat) persoonsgegevens van de betrokkene of van een andere natuurlijke persoon mag gebruiken. Je moet wel handelen in het belang van een individuele persoon.

Ten slotte blijft nog **het gewettigd belang van de verantwoordelijke of van een derde partij** over. Dit is niet van toepassing op publieke autoriteiten. Wanneer je deze rechtsgrond inroept, moet je dit altijd verduidelijken en moet je je belangen goed afwegen tegen het recht op privacy van de betrokkenen.

Zowel in het eigen register als in de privacyverklaring die je opstelt als toelichting voor de betrokkenen moet je dit duidelijk uitleggen en aantonen. Louter economisch belang is niet langer voldoende als verantwoording. En de verwerking moet wel degelijk noodzakelijk zijn. Dit is in elk geval de zwakste rechtsgrond uit het rijtje. Maar in de B2C wereld zal het waarschijnlijk de meest gebruikte zijn voor alles wat geen contractuele basis heeft.

De GDPR vraagt expliciet extra aandacht voor de verwerking van gegevens over kinderen (tot de leeftijd van 16 jaar). Daarvoor is toestemming van de ouders nodig, wat niet zo gemakkelijk te organiseren is.

Als het gaat om de verwerking van speciale categorieën[15] van persoonsgegevens (zie voor de definitie hoofdstuk 1.2) gelden nog striktere regels. Dergelijke verwerking is verboden, behalve in bepaalde gevallen, die door de GDPR worden opgesomd.

We overlopen ze kort:

- Indien de betrokkene expliciet zijn toestemming heeft gegeven.
- Als het gaat om gegevens die reeds publiek beschikbaar zijn omdat ze manifest door de betrokkene zelf openbaar gemaakt zijn.
- Op grond van tewerkstellingswetgeving (allerhande gegevens moeten verwerkt worden in het kader van sociale zekerheid, wettelijke verplichtingen en contractuele overeenkomsten).
- In zaken van levensbelang, als de betrokkene niet in staat is zijn toestemming te geven (hier gaat het vaak precies over het gebruiken of doorgeven van medische gegevens).

[15] Artikel 9 : Overweging 51-56

- Voor vzw's of organisaties voor een goed doel, voor zover het gaat om wettig gebruik van gegevens over leden, vroegere leden of personen met wie ze regelmatig contact hebben.
- Voor verenigingen, vakbonden of politieke en religieuze organisaties (met politieke, filosofische of religieuze doeleinden).
- Gegevens over misdrijven of strafrechtelijke zaken kunnen enkel verwerkt worden door publieke autoriteiten of in gevallen die door de wetgeving (Europees of landelijk) zijn voorzien. Elk land kan daarbij zijn eigen beperkingen opleggen. Strafrecht is trouwens een nationale materie en wordt niet geregeld door de GDPR.
- Indien de gegevens noodzakelijk zijn in het kader van rechtszaken.
- In een aantal gevallen omwille van het algemeen belang:

    - Bij substantieel algemeen belang, en gedekt door Europese Unie (EU) of landelijke wetgeving, die ook de rechten van het individu beschermt;
    - In het kader van de gezondheidszorg (diagnoses door medische professionals; gegevens voor de organisatie van gezondheidszorg of sociale zekerheid, assessments van de gezondheid van werknemers; onderzoek van geneesmiddelen);
    - Gegevens nodig voor wetenschappelijk of historisch onderzoek of archivering, waarbij je de nodige beschermingsmaatregelen moet nemen (de resultaten van onderzoek kunnen bijvoorbeeld geanonimiseerd of gepseudonimiseerd worden).

Er is steeds een gewichtige reden nodig om persoonsgegevens te verwerken. In de volgende hoofdstukken verdiepen we ons nog verder in de toestemming van de betrokkene en in het gewettigd belang van de verantwoordelijke als rechtsgrond.

4.2 Toestemming van de betrokkene

De beste basis om legaal persoonsgegevens te verwerken is toestemming[16] krijgen van de betrokkene zelf. In de praktijk is dit echter lang niet zo vanzelfsprekend.

Doordat die goedkeuring te allen tijde kan worden ingetrokken, houdt deze rechtsgrond ook een onzekerheid in.

[16] Artikel 4.11; Artikel 7-8 : Overweging 32-33,38,42-43

De toestemming heeft al lang een plaats in de privacywetgeving, maar de regels zijn door de jaren steeds strenger geworden. Aanvankelijk kon je nog een soort stilzwijgende goedkeuring afdwingen, vaak als onderdeel van een ruimer contract en zonder een welbepaalde doelstelling. Vervolgens kwam de verplichting om het intrekken van deze goedkeuring mogelijk te maken (de zogenaamde 'opt out'). De GDPR legt nu een hele reeks voorwaarden vast die je moet vervullen om van een rechtsgeldige toestemming te kunnen spreken ('opt in').

De toestemming moet vrijwillig, actief, geïnformeerd en duidelijk gespecificeerd gegeven worden en moet even gemakkelijk weer ingetrokken kunnen worden.

Vrijwillig

Toestemming van de betrokkene kan niet als rechtsgrond gebruikt worden als er geen evenwichtige verhouding is tussen de verantwoordelijke en de betrokkene. Dit geldt bijvoorbeeld voor de relatie tussen werknemer en werkgever. De werknemer verkeert immers meestal niet in de positie om te weigeren.

De toestemming mag ook niet worden gekoppeld aan het verlenen van een service, behalve als de gegevens direct noodzakelijk zijn om de overeenkomst te kunnen uitvoeren.

In dat geval is de rechtsgrond echter de contractuele noodzaak en wordt er voor de duidelijkheid ook beter geen toestemming gevraagd.

Goedkeuring voor gegevensgebruik in latere marketing- en reclamecampagnes mag ook geen onderdeel zijn van een af te sluiten contract of van algemene voorwaarden. Ze is voor de GDPR enkel geldig als beide handelingen gescheiden kunnen gebeuren. De goedkeuring mag ook niet gekoppeld worden aan andere zaken zoals kortingen. 5% korting of een geschenk in ruil voor je toestemming mag niet.

Actief

De betrokkene moet zelf een duidelijk statement maken of een actieve handeling verrichten om aan te geven dat hij zijn toestemming verleent voor een welbepaalde verwerking. Elke geschikte werkwijze of methode is hiervoor toegelaten.

De GDPR somt zelf de meest gangbare methoden op: mondeling of schriftelijk je toestemming geven, een check box aanklikken of een instelling binnen een browser of een app activeren. Nieuw is dat de GDPR expliciet uitsluit dat dit stilzwijgend of door inactiviteit zou gebeuren. Een vooraf aangevinkte check box bijvoorbeeld is uit den boze. Een 'opt-out' functie of een 'unsubscribe' knop niet gebruiken is evenmin een geldige toestemming. Dit is een erg belangrijke voorwaarde voor alle organisaties die direct marketingcampagnes opzetten.

Geïnformeerd

De betrokkene moet vooraleer je hem om zijn toestemming vraagt, omstandige informatie krijgen over de identiteit van de verantwoordelijke, de geplande verwerkingen, de doelstelling en de wettelijke grond en over de genomen maatregelen om zijn data te beschermen. Dit moet gebeuren op een eerlijke manier en je moet heldere en eenvoudige taal gebruiken. Er moet een duidelijke lijn zijn tussen de doelstelling, de gegevens die precies daarvoor nodig zijn en de te geven goedkeuring. Je kan hiervoor een gedetailleerd uitgewerkte privacyverklaring gebruiken. Welke informatie daarin moet staan en hoe je die best beschikbaar stelt aan de betrokkenen, behandelen we uitvoerig in een later hoofdstuk.

Specifiek en zonder ambiguïteit

Toestemming tot het verwerken van persoonsgegevens wordt altijd gegeven voor een duidelijk doel. De verantwoordelijke mag de gegevens dan ook niet voor andere doeleinden aanwenden, tenzij de nieuwe doelstelling heel dicht aanleunt bij de oorspronkelijke.

Een goed voorbeeld is het contacteren van een vroegere of bestaande klant om hem te informeren over een product of dienst, verwant aan wat hij vroeger al heeft aangekocht.

Speciale aandacht is nodig als je overweegt gegevens op een andere manier te combineren of voor een totaal ander doel te gebruiken. Datamining is in deze context een probleem. Deze techniek wordt onder meer voor marketing geregeld aangewend om binnen grote hoeveelheden informatie mogelijke patronen of onverwachte verbanden te ontdekken, zodat er geen vooropgesteld doel is. De GDPR laat in gevallen van hergebruik van data wel ruimte voor een versoepeling. Je kan de expliciete goedkeuring van de betrokkene alsnog vragen bij het eerstvolgende gebruik van de data.

Toestemming is intrekbaar

In elk geval moet je de betrokkene informeren dat hij steeds zijn toestemming kan intrekken. Dit moet kunnen met een eenvoudige handeling, even gemakkelijk als het geven van de toestemming zelf. De GDPR legt deze verplichting nu overduidelijk bij de verantwoordelijke.

Hoewel deze aanpak fair en logisch lijkt, is de praktische uitwerking niet altijd even evident. Zeker omdat de GDPR verplicht dat de verantwoordelijke duidelijk moet kunnen aantonen dat de betrokkenen hun toestemming wel degelijk gaven.

4.3 Toestemming of gewettigd belang?

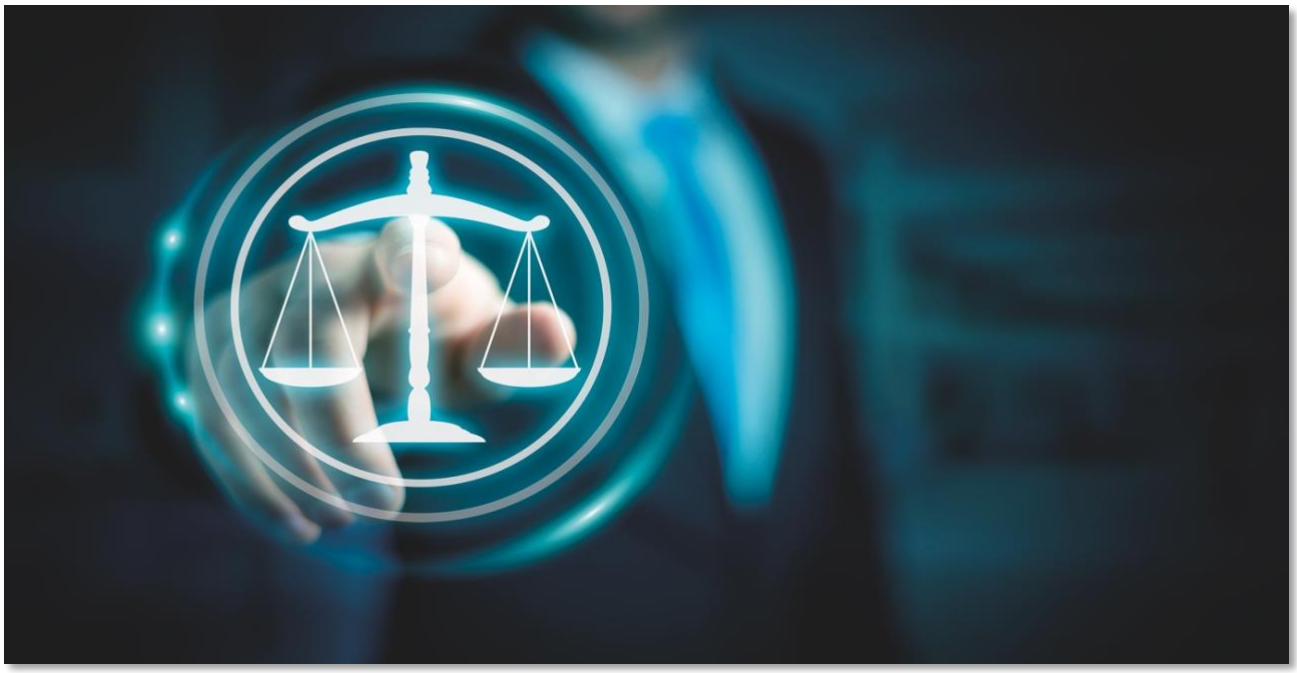
We hebben in de vorige hoofdstukken de verschillende mogelijke rechtsgronden voor het verwerken van persoonsgegevens voorgesteld. In een aantal gevallen kunnen meerdere rechtsgronden[17] ingeroepen worden. Maar hoe kies je de beste grond om je verwerking te verantwoorden?

Deze vraag is minder gemakkelijk te beantwoorden dan het misschien lijkt. Toch is het belangrijk hierbij stil te staan, want er zijn wel degelijk gevolgen verbonden aan de keuze. De ene rechtsgrond geeft je op lange termijn namelijk meer zekerheid dan de andere.

Maar omschakelen tussen meerdere mogelijkheden schept dan weer verwarring en kan de indruk wekken dat je de betrokkenen wil misleiden.

[17] Artikel 6-9 : Overweging 47-49

Zolang het over gegevens gaat die verwerkt worden om een contract uit te voeren (zoals bijvoorbeeld contactgegevens voor orders, leveringen of serviceverlening en facturatie) of in het kader van wettelijke verplichtingen, hoef je niet te twijfelen. De keuze maken tussen toestemming van de betrokkene of het inroepen van gewettigd belang is echter een stuk moeilijker.



Toestemming van de betrokkenen vragen lijkt altijd een goede optie, maar dit brengt ook risico's met zich mee. Als je toestemming vraagt en je krijgt die niet, dan mag je de gegevens uiteraard niet meer verwerken. Stel dat je iedere persoon in een bestand voor een marketingcampagne aanschrijft of mailt en hen vraagt hun expliciete toestemming te geven om hen in de toekomst te contacteren. De respons op dergelijke actie ligt misschien rond de 10 procent. Het gevolg is dan dat je het overgrote deel van je contacten niet meer mag gebruiken.

In alle gevallen waar je kunt aantonen dat je die toestemming wel degelijk hebt gekregen, zit je natuurlijk veilig. Je creëert op die manier ook een goed imago, door open te communiceren over je intenties en rekening te houden met de voorkeur van je contactpersonen. Maar het hindert wel de ruime verspreiding van je campagnes en maakt het erg moeilijk om nieuwe bestemmelingen toe te voegen. De kans bestaat altijd dat een betrokkene later nog op zijn beslissing terugkomt en zijn goedkeuring intrekt, waardoor de contactenbasis nog verder afbrokkelt.

Welke alternatieven heb je dan? Je kan altijd het gewettigd belang van je organisatie als rechtsgrond inroepen.

Een commerciële organisatie – om hetzelfde voorbeeld van de marketingcampagnes te nemen – kan immers niet functioneren zonder de mogelijkheid haar producten of diensten voor te stellen en aan te prijzen. Zoals eerder al vermeld, moet je dan je dossier met zorg opbouwen. Beperk om te beginnen de te verwerken gegevens tot wat strikt noodzakelijk is.

Met minder informatie is de kans op een ernstige schending van de privacy automatisch kleiner. Een bestand met louter contactgegevens weegt minder zwaar dan een grote verzameling data die deels gevoelig zijn.

Neem vervolgens de nodige maatregelen om deze gegevens te beschermen en de vertrouwelijkheid te verzekeren. Toon aan dat de verzamelde gegevens niet voor een ander doel gebruikt kunnen worden.

Op die manier bewaar je het evenwicht tussen de belangen van de betrokkenen en die van je eigen organisatie. De argumentatie die je volgt, leg je best beknopt (of omstandiger) vast in je register. Bij mogelijke betwistingen kan je dan altijd aantonen dat je te goeder trouw handelde en dat je de juiste overwegingen hebt gemaakt.

Geen van deze maatregelen voorkomt echter dat gewettigd belang als rechtsgrond altijd kan aangevochten worden. Een betrokkene die zich onrechtmatig behandeld voelt of een concurrent die vindt dat je er oneerlijke praktijken op nahoudt, kan een klacht indienen bij de Belgische gegevensbeschermingsautoriteit of de Autoriteit Persoonsgegevens in Nederland.

Dit kan leiden tot een onderzoek en eventueel een rechtszaak. Wat het resultaat hiervan zal zijn, hangt af van de interpretatie van de concrete feiten door de auditors of de rechter en die kan uiteraard anders zijn dan je eigen inschattingen. Een afwijkende uitspraak kan ertoe leiden dat je een boete krijgt, de verwerking niet mag verderzetten en mogelijk een schadevergoeding moet betalen. Bij het bepalen van de uitspraak en de corrigerende maatregelen zal de Belgische gegevensbeschermingsautoriteit wel rekening houden met de algemene situatie. Als een organisatie met geen enkel aspect van de privacywetgeving in orde is, zullen de feiten zwaarder wegen. Als je de nodige maatregelen genomen hebt en duidelijk kunt aantonen op grond van welke redeneringen je bepaalde verwerkingen gerechtvaardigd acht, zullen de feiten je minder zwaar aangerekend worden.

We zijn ons ervan bewust dat we hiermee geen duidelijk antwoord of richtlijn hebben gegeven.

Maar privacy is een recht dat moet afgewogen worden tegenover andere rechten en zal altijd een kwestie van interpretatie en discussie zijn. Met gezond verstand en een eerlijke, open benadering kom je al een heel eind. Daarna moet je de gevolgde zienswijze duidelijk communiceren en goed documenteren. Uiteraard moet je wel zorgen dat je in het hele verwerkingsproces de verwachte beveiligingsmaatregelen neemt om de risico's op inbreuken te beperken.

5. Transparantie

5.1 Wat is een privacyverklaring en wat moet erin staan?

In de vorige hoofdstukken hebben we het uitvoerig gehad over het register van verwerkingen van persoonsgegevens. Daarin neem je op welke persoonsgegevens in je organisatie verwerkt worden, met welk doel dit gebeurt en wat de rechtsgrond daarvoor is. Als je organisatie de GDPR wil naleven, moet je zo'n register hebben. De bruikbaarheid van dit register gaat echter veel verder. Je kunt het perfect als vertrekpunt nemen voor een risicoanalyse en voor een overzicht van de beschermingsmaatregelen en interne procedures van je organisatie. Daarop komen we later in deze publicatie nog terug. Anderzijds levert een goed bijgehouden register ook de juiste input om de betrokkenen te informeren over de verwerking van hun gegevens. Dat laatste bespreken we verder in dit hoofdstuk.

De GDPR vereist immers dat je open en transparant bent voor alle betrokkenen, met andere woorden voor alle personen van wie je gegevens gebruikt. Het is hun recht om te weten hoe je hun gegevens verwerkt. Een tekst waarin je als organisatie deze informatie publiek maakt, noemen we een 'privacyverklaring[18]'.

De GDPR legt vast welke informatie de betrokkene moet krijgen. Een goed opgestelde Privacyverklaring moet dus elk van deze items behandelen.

- De **verantwoordelijke voor de gegevensverwerking** moet zichzelf duidelijk kenbaar maken, met de exacte naam van de firma of de organisatie en met het volledige adres van de zetel. Als de organisatie een Data Protection Officer (DPO) heeft aangesteld, moet de privacyverklaring ook vermelden hoe deze gecontacteerd kan worden. Het is niet nodig de naam van deze persoon te geven, maar wel minstens een adres, telefoonnummer of mailadres waarmee hij bereikbaar is. Als er geen DPO is, moet evenzeer verwezen worden naar een contactpunt.
- Het belangrijkste deel van de verklaring is **de opsomming van de verwerkingen** van persoonsgegevens die je organisatie doet. Per doelstelling moet je voldoende in detail gaan. Je geeft telkens aan met welke **bedoeling** bepaalde gegevens verzameld worden, welke **categorieën** van gegevens je verwerkt en over welke categorieën van personen het gaat, welke **verwerkingen** er gebeuren en op welke rechtsgrond je je beroept om de verwerking te kunnen doen. Hiervoor kun je uiteraard putten uit het interne register, zodat je niets vergeet.

[18] Artikel 13-14 : Overweging 60-62

- Er moet ook duidelijkheid zijn over de **bestemmelingen**. Wie heeft toegang tot deze informatie? Aan wie wordt ze doorgegeven? Geef aan welke categorieën medewerkers intern bij de verwerking betrokken zijn en dus inzage hebben in de informatie. Vermeld of er externe partijen aan de verwerking deelnemen. Als de verzamelde informatie doorgegeven wordt aan derden, moet je dit zeker expliciet aangeven. Meestal gebeurt dit in algemene bewoordingen als 'zustermaatschappijen' of 'partners'.
  De GDPR gaat uit van zoveel mogelijk transparantie. Het is immers belangrijk dat de betrokkenen begrijpen waar hun gegevens terechtkomen. Uiteraard kan men niet verwachten dat je elke partner of leverancier met naam en toenaam opsomt.
- Vervolgens toon je aan dat er **voldoende beveiligingsmaatregelen** genomen zijn om de vertrouwelijkheid en integriteit van de data te verzekeren. Ook hier is het niet nodig alle technologie en procedures in detail uit de doeken te doen. Dat zou natuurlijk juist de beveiliging ondergraven. Maar de gevolgde principes en de manier waarop je deze intern kunt waarborgen, vermeld je best wel.
- Een specifieke vereiste is informatie over **de bewaartermijn van gegevens**. De GDPR zegt immers dat je persoonsgegevens alleen voor het gestelde doel mag gebruiken en dus ook niet langer mag bewaren dan nodig is voor dat doel. Bovendien moet je als verantwoordelijke instaan voor de kwaliteit van de gegevens. Dat houdt ook in dat ze niet verouderd zijn. Info over de bewaartijd vermeld je best specifiek per doel.
- Verder moet de privacyverklaring ook de **rechten van de betrokkene** duidelijk opsommen.
    - Als hij van oordeel is dat gegevens onrechtmatig verwerkt worden, kan hij altijd een klacht indienen bij de Belgische gegevensbeschermingsautoriteit;
    - Hij kan bij de verantwoordelijke informatie opvragen over de verwerkingen van zijn gegevens en je moet hem uitleggen welke procedure hij daarvoor kan volgen;
    - Hij kan inzage krijgen in de beschikbare informatie en deze desgewenst laten wijzigen of wissen.

- Ten slotte vraagt de GDPR dat je kenbaar maakt of je bepaalde **gegevens buiten de Europese Economische Ruimte (EER)** transporteert. In dat geval zijn er immers extra risico's voor de adequate bescherming van de gegevens en voor de rechten van de betrokkene. Denk maar aan de bevoegdheden van instanties als het National Security Agency (NSA) in de Verenigde Staten.
  Al naargelang het land waarnaar de gegevens uitgevoerd worden of de sector van de firma of organisatie, zijn er andere garanties. Dit is juridisch heel ingewikkelde materie. Meestal zal het volstaan te vermelden dat de gegevens binnen de Europese Economische Ruimte blijven en dus ten volle gedekt worden door de juridische bescherming van de GDPR. Als dat niet het geval is, moet je specificeren waar ze naartoe gaan en welke bescherming van toepassing is. De betrokkene kan dan zelf oordelen of zijn gegevens in voldoende mate vertrouwelijk zullen blijven.

De GDPR schrijft niet enkel voor welke inhoud een privacyverklaring moet bevatten maar geeft ook richtlijnen over de vorm en structuur. Het is belangrijk op welke manier je deze informatie communiceert aan de betrokkenen, op welk moment je ze aanbiedt en hoe je ze actueel houdt. Deze aspecten komen in het volgende hoofdstuk aan bod.

5.2 Hoe presenteer je een privacyverklaring best?

In het vorige hoofdstuk hebben we overlopen wat je allemaal moet opnemen in een privacyverklaring, zodat alle betrokkenen correct zijn ingelicht over de verwerkingen die er met hun data gebeuren. Op welke manier je dit doet, is ook belangrijk. De opstellers van de GDPR hebben hieraan specifiek aandacht besteed.

Als verantwoordelijke heb je de plicht deze informatie te verstrekken **in beknopte vorm en in heldere en begrijpelijke taal**[19]. In het verleden waren sommige firma's kampioen in het opstellen van loodzware teksten met voor gewone mensen onbegrijpelijke formuleringen, liefst tientallen pagina's lang. Op die manier ontmoedig je de gebruiker om het document werkelijk te lezen. Dit is het tegengestelde van transparantie. De GDPR verwacht dat je eenvoudige taal gebruikt, die zowat iedereen kan verstaan. In Nederland beveelt men expliciet taalniveau B1 aan. Dat is niveau lager onderwijs. Als je publiek ook uit kinderen bestaat, is het extra belangrijk dat je op een simpele en begrijpelijke manier uitlegt wat je doet met gegevens die zij doorgeven. Het is vaak de beste oplossing een aparte privacyverklaring voor kinderen op te stellen.

De transparantie is ook groter als je **eerst de hoofdlijnen** beknopt weergeeft en de tekst goed structureert. Je kan bijvoorbeeld elk onderwerp beschrijven in één zinnetje of een korte alinea en dan **de mogelijkheid** geven **om door te klikken** naar meer informatie. Zo vindt de gebruiker items snel terug en kan hij desgewenst daarop dieper ingaan. Het kan een goed idee zijn te werken met iconen, om zo nog eenvoudiger de boodschap over te brengen dan met louter tekst. Werkgroepen zijn al verschillende jaren bezig met het ontwikkelen van specifieke iconen, maar dit is ook een uitdaging.

Vergeet ook niet de privacyverklaring te **dateren en een versienummer** te geven. Dit soort teksten zijn immers levend. Er kunnen wijzigingen komen in de aard van de gegevens die je verwerkt, in de bestemmelingen of in de genomen beschermingsmaatregelen. Je tekst moet correcte en actuele informatie geven en zal dus regelmatig wijzigen. Eigenlijk horen de betrokkenen ook op de hoogte te zijn van deze wijzigingen. Je moet hen dus op zijn minst duidelijk maken dat de verklaring later kan veranderen. Nodig hen uit de pagina op je website regelmatig opnieuw te bezoeken. Het is nuttig oudere versies van je privacyverklaring bij te houden, zodat in geval van betwisting van een verwerking kan nagegaan worden welke informatie op het ogenblik van die verwerking beschikbaar was voor de betrokkenen.

[19] Artikel 12.1 : Overweging 58

Op welke plaats en in welke vorm je de privacyverklaring best kenbaar maakt, is afhankelijk van de omstandigheden. Zorg er zeker voor dat ze **gemakkelijk terug te vinden** is. Een privacyverklaring verstoppen tussen je algemene voorwaarden is te vermijden. De meest gangbare methode is een link vanaf de website, maar een privacyverklaring kan ook op papier of zelfs mondeling gecommuniceerd worden. Er zijn wel een aantal regels waarmee je rekening moet houden.

Als je op een website of in een toepassing persoonsgegevens door gebruikers laat invullen, dan moet je ervoor zorgen dat je de nodige informatie over de verwerking **vooraf** gegeven hebt.

Dit kan het best gebeuren door al in de introductie tot deze toepassing een verwijzing op te nemen naar de privacyverklaring. Op veel websites vind je dergelijke verwijzing in een balk onderaan elke pagina. Dat is natuurlijk minder specifiek en niet gerelateerd aan één bepaalde doelstelling.

Maar de info is dan wel vanaf het openen van je website meteen bereikbaar. Dit is belangrijk op websites die via cookies of andere tools info vergaren over het surfgedrag van bezoekers. Dit start immers bij het openen van de website, zodat de bezoeker hiervan meteen op de hoogte gebracht moet worden.

Het is zeker niet verkeerd om **meerdere privacy verklaringen** te maken, aangepast aan bepaalde doelgroepen. Je (potentiële) klantenzijn wellicht niet geïnteresseerd in de omgang van je organisatie met personeelsgegevens. Op die manier beperk je telkens ook de lengte van de tekst.

Tip:
De GDPR is een goede aanleiding voor elke organisatie **om het beleid rond het verwerken van personeelsgegevens** eens door te lichten en erover te communiceren binnen het bedrijf. Er circuleren meer gegevens over het personeel dan je denkt en sommige daarvan zijn gevoelig.

- Allerlei gegevens zijn nodig voor de loonverwerking (salaris, aanwezigheid, ziekteverzuim, samenstelling van het gezin). Voor veel bedrijven wordt deze informatie extern verwerkt door een sociaal secretariaat, dat dus de rol van dataverwerker krijgt. Voorts moeten voor de sociale zekerheid en de belastingadministratie gegevens doorgegeven worden aan de overheid.

- Verder bevatten de interne personeelsdossiers allerlei loopbaangegevens. Naar aanleiding van aanwervingen, evaluaties of promoties komt deze informatie ook buiten de personeelsdienst terecht.
  Het is belangrijk de procedures rond vertrouwelijkheid van deze gegevens nog eens op punt te stellen.

- Andere gegevens hebben betrekking op het gebruik van ICT-tools. Dit kan gaan van de inhoud van mails via useraccounts, gebruikersgroepen en autorisatieniveaus tot logs van het gebruik van toepassingen of het bezoeken van websites. Het is belangrijk om open te communiceren over de informatie die in logs wordt bijgehouden en het doel hiervan. Je moet ook duidelijk maken wat de werkgever wel en niet mag doen met deze informatie.

In grotere organisaties is dit materie die op de Ondernemingsraad moet besproken worden. Maar ook in kleinere firma's is het nodig de werknemers op de hoogte te stellen van alle verwerkingen van persoonsgegevens. Dit kan in de vorm van een interne privacyverklaring, die je in het arbeidsreglement opneemt of als een apart document verspreidt, op papier of digitaal. Het is geen slecht idee om die tekst voor kennisgeving te laten ondertekenen door je werknemers.

Het zal soms wat creativiteit vergen, maar met enige goede wil kan elke organisatie duidelijkheid scheppen over de verwerkingen van persoonsgegevens die zij doen en de redenen waarom deze nodig zijn. Transparant zijn is immers een basisvereiste. In de volgende hoofdstukken zullen we uitleggen wat de GDPR bedoelt met adequate beschermingsmaatregelen voor de te verwerken persoonsgegevens. Dit kan voor veel bedrijven een grote uitdaging worden.

6. Beveiliging van persoonsgegevens

6.1 Adequate beveiliging van persoonsgegevens

Tot hiertoe hebben we het in deze publicatie vooral gehad over de GDPR-richtlijnen voor het eigenlijke verwerken van persoonsgegevens. Onder welke voorwaarden mag je gegevens verwerken? Hoe zorg je voor de juiste communicatie met de betrokkenen? Daarnaast schrijft de GDPR ook voor dat je de gegevens afdoende moet beschermen tegen risico's, zowel tijdens de verwerking als daarbuiten.

De plicht tot informatiebeveiliging[20] bestond natuurlijk al in de vroegere wetgeving. Nieuw in de GDPR is dat niet alleen de verantwoordelijke voor de verwerking aansprakelijk is, maar evenzeer elke verwerker die persoonsgegevens behandelt in opdracht van een verantwoordelijke.

Om duidelijk te maken hoe je aan deze verplichting kunt voldoen, moeten we even stilstaan bij wat informatiebeveiliging is. Grotere organisaties of firma's die systematisch vertrouwelijke data van hun klanten behandelen, zijn hiermee vertrouwd. Er zijn verschillende standaarden voor informatiebeveiliging, waarvan **ISO 27001** de meest bekende is. Een heel arsenaal aan beleidsnota's, procedures en werkinstructies ondersteunen organisaties en hun management hierbij. Dit is een 'wetenschap' op zich.

[20] Artikel 24.2 en 25; Artikel 32

Een informatiebeveiligingsprogramma helpt je om systematisch de nodige stappen te nemen. Je moet de specifieke risico's die de informatie loopt, kennen. Je moet proberen deze risico's weg te werken, in te perken of de impact ervan te verminderen.

Welke maatregelen precies zorgen voor adequate beveiliging, zegt de GDPR niet. Dit is niet onlogisch, want de gepaste werkwijze hangt van veel elementen af.

Aan de ene kant zijn de risico's niet altijd dezelfde:

- Zowel de aard van de gegevens (speciale categorieën, gevoelige data of identificatiegegevens tegenover quasi-publieke gegevens) als de hoeveelheid bepalen de impact van een eventueel datalek.
- De aard van de verwerking zelf kan bepaalde risico's inhouden. Zo moet er extra aandacht gaan naar automatische gegevensanalyses waarop beslissingen gebaseerd zijn.
- Gegevensuitwisseling en transport van data kunnen voor extra risico's zorgen.
- De inschakeling van derden bij de verwerking kan een bijkomende bedreiging zijn.
- Buiten Europa (eigenlijk buiten de EER) geldt niet dezelfde bescherming.
- De bewaartermijn van gegevens kan eveneens een rol spelen.

Anderzijds staan wetenschap en technologie ook niet stil. Daardoor is wat vandaag een adequate beveiliging is, dat binnen twee jaar wellicht niet meer.

Het komt er dus op aan een evenwicht te vinden. De kosten en inspanningen om bepaalde maatregelen te nemen moeten in verhouding zijn tot de aard van de data en de schade die kan optreden als er iets misloopt.

Grotere organisaties gebruiken hiervoor ook nu al een hele reeks procedures. Ze formuleren het beleid rond informatiebeveiliging en hebben een informatie management systeem opgezet. Ze inventariseren de risico's en wegen af of ze aanvaardbaar zijn. Ze stellen procedures en instructies op.

Ze voeren controles uit en laten het systeem extern auditen. Ze analyseren incidenten en trekken lessen uit de actuele werking om deze te verbeteren. Al deze stappen zitten bijvoorbeeld in de standaarden van ISO 27001 verwerkt.

We overlopen even de basisprincipes.

In de eerste plaats moet je weten tegen welke bedreigingen persoonsgegevens, net als andere vertrouwelijke gegevens, beschermd moeten worden. Meestal gebruikt men hierbij het letterwoord CIA - elke overeenkomst met de Amerikaanse organisatie is toevallig. CIA staat hier voor Confidentiality – Integrity – Availability. Informatiebeveiliging garandeert de vertrouwelijkheid, de integriteit en de beschikbaarheid van data.

- De **vertrouwelijkheid** garanderen is ervoor zorgen dat gegevens niet openbaar worden en niet terechtkomen bij mensen voor wie ze niet bestemd zijn. We kennen allemaal de opvallende voorbeelden van gestolen creditkaartgegevens of van vertrouwelijke documenten die publiek gemaakt worden door hackers.

Maar er zijn ook kleinschaliger datalekken, zoals een brief die in de verkeerde brievenbus terechtkomt of een mail die bewust of per ongeluk naar de verkeerde bestemmeling is gestuurd.

- Beschermen van de **integriteit** van data betekent dat de data niet onterecht gewijzigd of gewist mogen worden. Vervalsing kan regelrechte fraude zijn en hackers kunnen data manipuleren, maar veel vaker liggen onbedoelde wijzigingen door menselijke fouten in software of bij het configureren van systemen of toepassingen aan de basis.
- Ten slotte moet je de **beschikbaarheid** van de data garanderen. Maatregelen als back-ups of een disaster recovery plan moeten voorkomen dat gegevens verloren gaan of dat ze niet kunnen geraadpleegd of verwerkt worden op het ogenblik dat dit nodig is.

Als je al een dergelijk informatie management systeem hebt, zijn er niet zo veel extra acties nodig om je informatiebeveiliging in orde te brengen voor de GDPR. Uiteraard moet je ervoor zorgen dat alle persoonsgegevens de classificatie 'vertrouwelijk' krijgen en dat de procedures voor het behandelen van vertrouwelijke gegevens erop van toepassing zijn. Vermoedelijk zijn er enkele extra procedures nodig om specifieke verwerkingen van persoonsgegevens beter te regelen, maar voor het overige is het algemene kader van toepassing.

De uitdaging is veel groter voor een firma of een organisatie die niet met informatiebeveiliging vertrouwd is. Daarom proberen we in de volgende hoofdstukken wat tips te geven over informatiebeveiliging in een kleine organisatie. Hoe kun je op een pragmatische manier en met gezond verstand haalbare procedures uitwerken en maatregelen nemen om het risico op incidenten met persoonsgegevens tot een minimum te beperken? En hoe kun je aantonen dat je dit op een adequate manier hebt gedaan?

6.2 Risicoanalyse van persoonsgegevens

De GDPR legt veel nadruk op de verplichting voor elke verantwoordelijke of verwerker van persoonsgegevens om afdoende bescherming te bieden voor de vertrouwelijkheid, de integriteit en de beschikbaar van de data. Ook als je niet beschikt over gespecialiseerd personeel, is het perfect mogelijk hieraan te voldoen. Je kan dezelfde stappen doorlopen op een eenvoudigere manier.

Alle maatregelen gaan uit van een risicoanalyse[21]. Dit klinkt moeilijk en gewichtig, maar hoeft helemaal niet zo te zijn. Neem gewoon je register van verwerkingen van persoonsgegevens (zie hoofdstuk 3) en overloop dit stap voor stap. Stel jezelf een paar gerichte vragen.

Voeg aan je register twee extra kolommen toe. Daarin formuleer je welke risico's aan elke specifieke verwerking verbonden zijn en met welke maatregelen je deze kunt beperken.

We sommen een paar simpele voorbeelden op, die in je eigen register waarschijnlijk ook voorkomen. Je beschikt over een verzameling contactgegevens van mensen die je graag af en toe informatie doorstuurt over je producten en diensten. Je houdt uiteraard hun naam en adres bij maar ook hun bedrijf, hun functie en misschien info over hun studies, hun hobby's, hun interessegebieden. Daarnaast heb je allerlei gegevens over je eigen personeel. Je houdt hun cv bij en de verslagen van hun jaarlijkse evaluatie. Je geeft elke maand door aan het sociaal secretariaat wie wanneer verlof neemt of ziek is. Je moet de samenstelling van hun gezin kennen, want de bedrijfsvoorheffing moet berekend worden. Misschien filmen je bewakingscamera's iedereen bij het binnenkomen en weggaan. Er zijn geen omgevingen denkbaar waar helemaal geen persoonsgegevens verwerkt worden.

Welke risico's zijn er voor de veiligheid van deze informatie? Veel hangt af van de manier waarop je de gegevens bewaart. In de vakterminologie spreken we van 'de gebruikte technologie'.

- Werk je met papieren dossiers, dan is de vraag of de 'fichebak' en de 'mappen' open en bloot op je bureau staan of op slot in een kast. Het is dan van belang wie toegang heeft tot je kantoor en wie bij de sleutel van de kast kan. Sluit je de deur als je weggaat? Ruim je op?
- Als je een bestand op computer bijhoudt, zijn de vragen in feite dezelfde, maar de antwoorden iets complexer. Misschien werk je lokaal op een laptop. Staat er een wachtwoord op? Ben je zelf de enige die dit wachtwoord kent? Zitten de vertrouwelijke persoonsgegevens in een bestand waarop je een wachtwoord hebt gezet? Als je je laptop meeneemt buiten het bedrijf, is hij dan extra beschermd? Laat je hem soms achter in de wagen? Waar bewaar je hem thuis?
- Als de gegevens niet lokaal worden opgeslagen, maar op een server, dan is de situatie weer verschillend. Hebben alle gebruikers van de server toegang tot alle data? Is dat eigenlijk nodig?

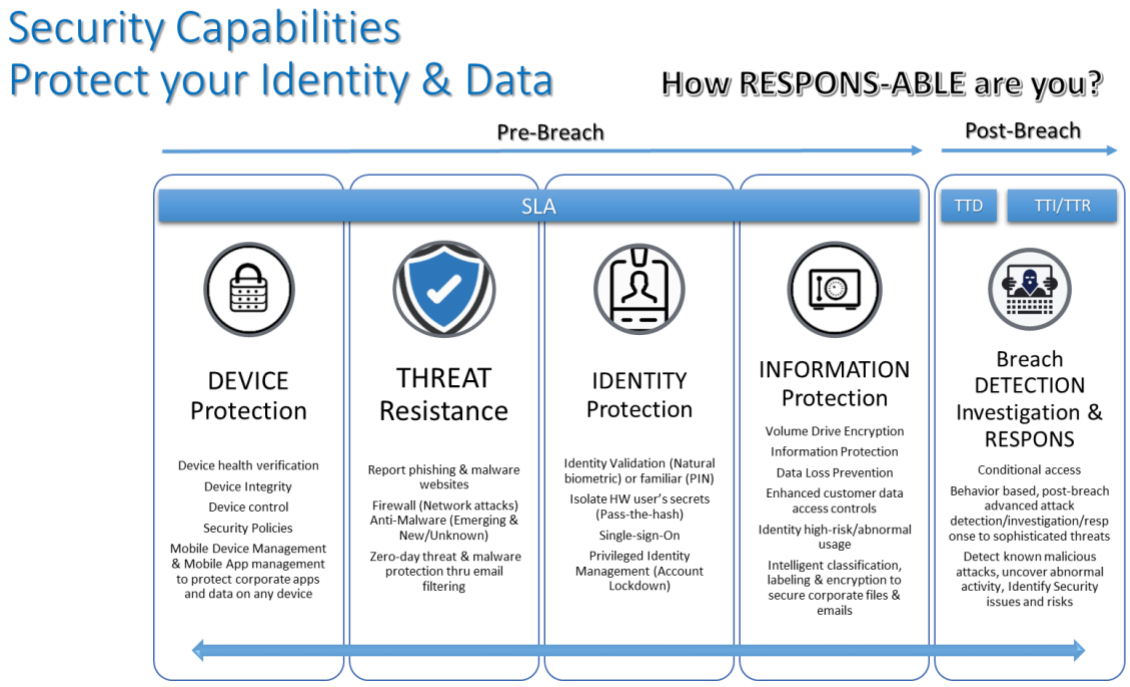
[21] Artikel 32; Artikel 35-36 : Overweging 75-76, 84, 89-95

Kun je de server niet in zones opsplitsen en andere autorisaties toekennen aan verschillende gebruikers of groepen? Worden er back-ups gemaakt van de server en waar worden die bewaard? Is er een IT-firma die het serverpark onderhoudt?
Hebben zij toegang tot alle data? Is met hen afgesproken wat ze wel en niet mogen doen, ook al hebben ze in feite alle rechten (omdat ze die voor hun taak nodig hebben)?

- Staan de data misschien in de 'Cloud'? Waar bevinden ze zich dan en wie heeft er toegang toe? Welke garanties geeft de Cloud provider? Worden data misschien in het buitenland geplaatst? Bevinden ze zich buiten de Europese Economische Ruimte en dus wat verder af van de bescherming van de GDPR? Verloopt de transmissie van data veilig?
- Worden de beelden van de beveiligingscamera's opgeslagen en bewaard? Hoe lang hou je ze bij? Wie kan ze bekijken en in welke omstandigheden worden ze effectief geraadpleegd?

Zoals de gestelde vragen al suggereren, kun je in elk van deze situaties maatregelen nemen om de kans op inbreuken sterk te verminderen. De voorbeelden tonen ook aan dat de risico's verschillend zijn naargelang de precieze inhoud van de bestanden.

Als het bij louter contactgegevens blijft, heeft een schending van de vertrouwelijkheid geen grote impact. Maar dat is helemaal anders als het over sommige personeelsgegevens gaat. Ook als je bijvoorbeeld in de gezondheidszorg werkt en gevoelige data van patiënten of cliënten bijhoudt, wat neerkomt op medische gegevens, is een veel striktere beveiliging nodig, precies omdat een inbreuk op de vertrouwelijkheid of de integriteit veel zwaardere gevolgen kan hebben. Afhankelijk van de omvang van de database wordt de impact ook groter naarmate het over de gegevens van meer mensen gaat. De maatregelen die je neemt in relatie tot elk van de opgesomde risico's, moeten altijd in evenwicht zijn met de inschatting van het risico.

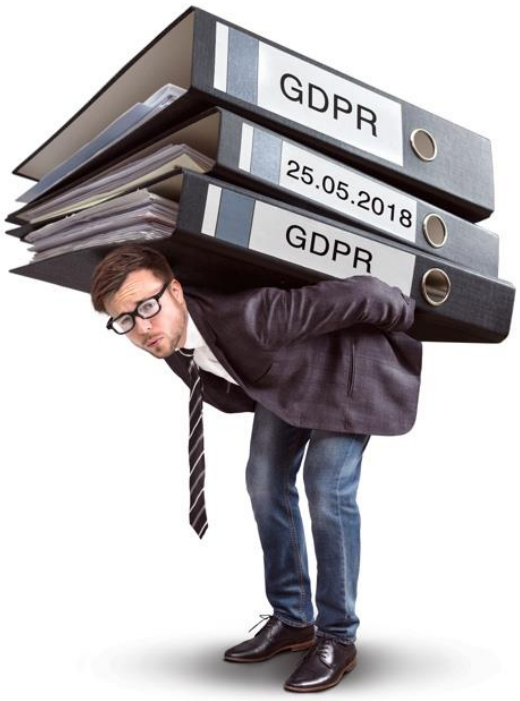


Het is dan ook logisch dat de GDPR grotere verplichtingen oplegt aan iedereen die speciale categorieën van gegevens gebruikt of aan elke organisatie die systematisch persoonsgegevens verwerkt als kernactiviteit. In sommige gevallen moet een formele 'dataprivacy impact analyse' (DPIA) worden opgesteld en voorgelegd aan de Belgische gegevensbeschermingsautoriteit voordat de verwerking start.

Los daarvan is het voor elke firma of organisatie raadzaam in grote lijnen dezelfde oefening te doen. Om op elk gewenst moment te kunnen aantonen dat je bewust met persoonsgegevens omgaat, is het aangewezen de bevindingen van deze analyse vast te leggen.

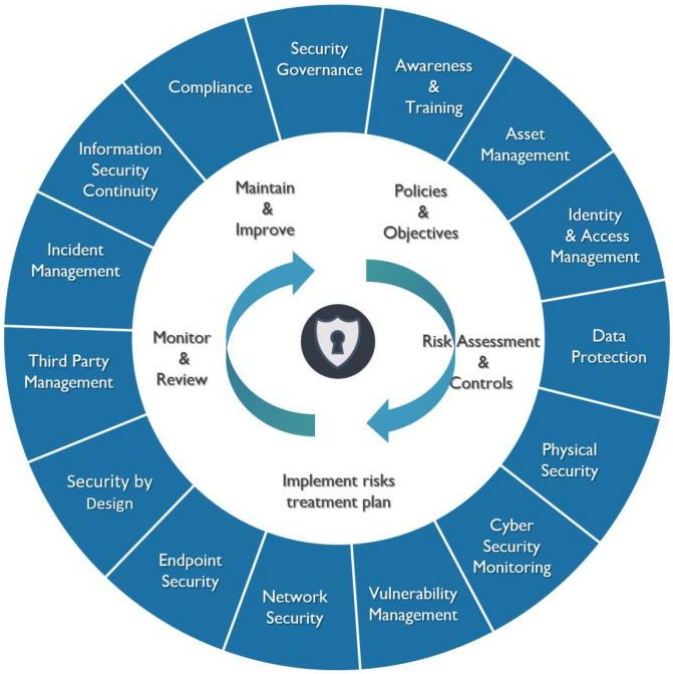
Gespecialiseerde software of methodologieën kunnen daarbij natuurlijk helpen, maar in veel gevallen is dat helemaal niet nodig. De reeds vermelde twee kolommen, die je kunt laten aansluiten bij een eenvoudig register van verwerkingen van persoonsgegevens, betekenen al heel veel.

In het volgende hoofdstuk gaan we dieper in op de verschillende domeinen waarin je beschermingsmaatregelen kunt nemen om veilig persoonsgegevens te bewaren en te verwerken.



6.3 Maatregelen voor de bescherming van persoonsgegevens

In het vorige hoofdstuk bespraken we het belang van een impactanalyse. De omvang van het risico bepaalt welke beveiligingsmaatregelen[22] noodzakelijk zijn. Nu komen de maatregelen zelf aan bod. Het is duidelijk dat een kleine firma dit anders zal aanpakken dan een grote. Toch is het leerzaam het stramien van een systeem als ISO 27001 kort voor te stellen. De gedachtegang en de logica die je moet volgen, blijft immers dezelfde.



De eerste blokken binnen ISO 27001 gaan over **beleid en organisatie**. Je moet de uitgangspunten van je beleid formuleren. Twee zinnen kunnen hiervoor volstaan. Het gebruik van persoonsgegevens moet legaal zijn en een gewettigd doel hebben en je moet de gegevens adequaat beschermen. Dit beleid vormgeven is de verantwoordelijkheid van de bedrijfsleider. Hij kan die taak delegeren, maar hij blijft verantwoordelijk en hij moet ook jaarlijks de doelmatigheid van het beleid beoordelen.

Bij het verdelen van die taken horen ook de bijhorende verantwoordelijkheden in het kader van gegevensbeveiliging binnen maar ook buiten je organisatie. Daarom is het aan te raden een kernteam op te richten, want de bedrijfsleider kan dit niet allemaal alleen beheren en bewaken.

[22] Artikel 32 : Overweging 77-78

Hij zal zich dan vooral kunnen richten op de sturing van het kernteam, die op hun beurt alle informatiedragers in kaart brengen door middel van een zo accuraat mogelijke inventarisatie die telkens zal worden bijgewerkt en waar nodig aangepast in functie van het gebruik. Middels deze lijst kan men starten met een risicoanalyse die later zal worden gebruikt om de nodige 'controles' te voorzien om het risico van gegevensverlies te kunnen beperken.

Daarna volgen **maatregelen in een aantal domeinen**, die in elk type bedrijf of organisatie op een of andere manier invulling moeten krijgen.

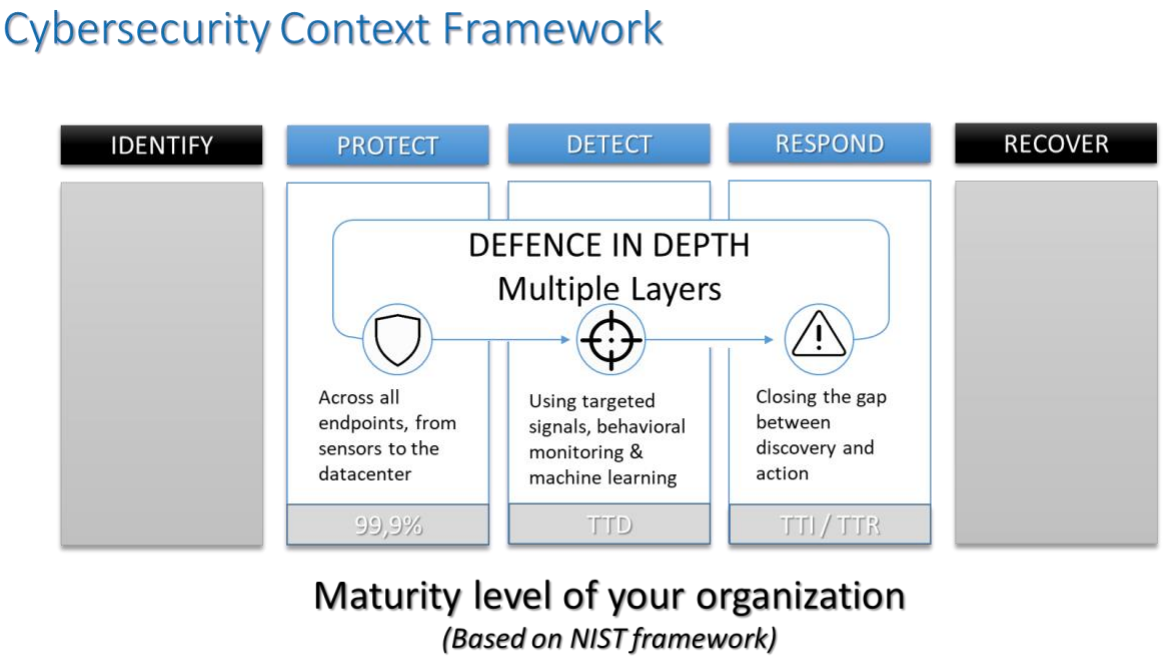
- Personeel (screening/ training & awareness/ uit dienst)
    - Let bij aanwervingen op de verantwoordelijkheidszin van je medewerkers.
    - Als je gevoelige gegevens verwerkt, vraag dan een uittreksel uit het strafregister (dat je dan vervolgens zelf ook als gevoelige informatie moet behandelen!).
    - Neem in de arbeidsovereenkomst een vertrouwelijkheidsclausule op. Dat kan één simpele zin zijn: 'Alle persoonsgegevens die je gebruikt in je werkomgeving, zijn vertrouwelijk en mag je enkel gebruiken voor de taak die je uitvoert'.
    - Train je medewerkers (en jezelf) regelmatig over dataprivacy.
    - Zorg ervoor dat een medewerker die uit dienst gaat, geen toegang meer heeft tot data en geen bedrijfsmiddelen bijhoudt (ook geen data op papier of digitaal).
- Classificatie en gebruik van middelen
    - Stel een register van verwerkingen van persoonsgegevens op en vul dit aan met een risicoanalyse.
    - Let op met verwijderbare media (bijvoorbeeld geheugensticks met data) en met toestellen die afgevoerd worden. Voorkom dat data in verkeerde handen komen.
- Toegangsrechten
    - Stel wachtwoorden in die complex genoeg zijn en hou ze strikt persoonlijk.
    - Geef je medewerkers enkel toegang tot informatie die nodig is voor hun functie. Werk hiervoor met 'functiegroepen'.
    - Beperk de administratorrechten op systemen tot bevoegde personen.
- Cryptografie
    - De GDPR propageert expliciet encryptie van data als beschermingsmaatregel. Dit is zeker aangewezen bij het uitwisselen van data en bij langdurige bewaring.

    - Voorbeelden zijn het https-protocol op websites, het sftp-protocol voor datatransfers, email encryptie….
    - Een ICT-partner kan je hierbij helpen. Maar vergeet niet ook met die partner goede afspraken te maken, zodat hij geen nieuw veiligheidsrisico wordt!
- Fysieke beveiliging
    - Schakel de schermbeveiliging van je pc in als je niet op je plek zit.
    - Laat op het einde van de werkdag geen documenten rondslingeren (clean desk).
    - Stel een sleutelplan op voor burelen (en kasten).
    - Onderzoek of je nood hebt aan hekken, een alarmsysteem, camerabewaking of een badgesysteem (en aparte zones binnen je gebouwen).
    - Beveilig je apparatuur tegen stroomuitval. Voorkom pannes.
    - Begeleid altijd je bezoekers en geef hen richtlijnen omtrent vertrouwelijkheid.
    - Besteed extra aandacht aan de ruimten waar gevoelige data beschikbaar zijn, zoals een serverroom of een archief met vertrouwelijke dossiers.
- Netwerkbeveiliging
    - Bescherm je netwerk tegen risico's van buitenaf door een firewall, door virusprotectie en door content filtering.
    - Splits grotere netwerken op in zones. Voorkom uitval van systemen. Monitor en log de activiteiten op het netwerk.
- Veiligheidsmaatregelen bij het ontwikkelen van toepassingen of systemen
    - Scheid testomgeving en productie en werk een regeling uit voor overzettingen.
    - Denk altijd vooraf na over de beveiliging van systemen en test deze voor gebruik.
- Controle over verwerkingen door derden
    - Maak contractuele afspraken over beveiliging en dataprivacy met je leveranciers.
    - Beoordeel de goede werking bij je leverancier en volg deze regelmatig op.
- Continuïteit
    - Beperk de kans dat systemen uitvallen door goed onderhoud en door ontdubbeling.
    - Zorg voor veiligheidskopieën van gegevens en stel een plan op om je systemen te herstellen als er zich ernstige problemen voordoen.

- Incidentbeheer
    - Registreer altijd incidenten die een risico inhouden op inbreuken tegen dataprivacy.
    - Meld altijd datalekken met impact, dat is verplicht.
- Audits
    - Controleer of je beveiliging afdoende is en laat ze evalueren.

De opgesomde maatregelen zijn uiteraard voorbeelden. De invulling zal bij iedereen wat verschillend zijn. Maar het overzicht kan een goede hulp zijn om aan alle domeinen te denken waar je actief risico's kunt beperken.

Enkele aspecten werken we in de volgende hoofdstukken nog verder uit, omdat de GDPR er extra aandacht aan besteedt. Dit is het geval voor de controle op onderaannemers of andere derde partijen en ook voor de verplichtingen die je hebt bij een datalek.



6.4 Risicobeheersing van onderaannemers/verwerkersovereenkomst

Zoals we in de vorige hoofdstukken hebben gezien is een van de domeinen waarin risico's kunnen ontstaan en waar dus beveiligingsmaatregelen genomen moeten worden, het inschakelen van onderaannemers[23].

De GDPR is hierin heel duidelijk.

Een onderaannemer is zelf aansprakelijk en heeft een aantal verplichtingen, maar de opdrachtgever die hem als verwerker inschakelt, behoudt altijd de verantwoordelijkheid. Hij moet zijn onderaannemer goed kiezen en staat in voor de legale uitvoering.

De opdrachtgever moet de opdracht duidelijk formuleren en kaderen en hij moet de correcte navolging van de instructies en van de wetgeving controleren, in het bijzonder de beveiliging.

De voorbije jaren is bij specialisten in informatiebeveiliging het besef gegroeid dat onderaannemers altijd een risico vormen. Het is dan ook niet verwonderlijk dat de GDPR hieraan veel aandacht besteedt. In de verschillende stadia van de samenwerking moeten bepaalde stappen gezet worden.

Bij het **selecteren van leveranciers** mag het aspect dataprivacy en informatiebeveiliging nooit ontbreken. De verantwoordelijke moet zich ervan vergewissen dat een onderaannemer die hij wil inschakelen zijn verplichtingen kent en er op een adequate manier aan voldoet. Een certificatie dat een bedrijf 'GDPR-compliant' is, bestaat niet en voor zover wij weten zijn er momenteel geen concrete plannen om dit in te voeren. De officiële instanties sporen wel de beroepsverenigingen aan om gedragscodes op te stellen, waarmee de ondertekenaars dan kunnen aantonen dat ze de regels kennen en willen volgen. Er duiken ook steeds meer vragenlijsten op, die gebruikt worden bij selectieprocedures en in aanbestedingsdossiers. Specifiek rond informatiebeveiliging zijn er natuurlijk wel certificaten, maar die zijn sterk toegespitst op grote organisaties en niet voor iedere firma of organisatie een haalbare kaart. Stel je toekomstige leverancier altijd vragen over zijn beleid rond informatiebeveiliging en over de maatregelen die van toepassing zijn. Laat dit bij de selectiecriteria meespelen. Vergeet ook niet de verzamelde documentatie bij te houden.

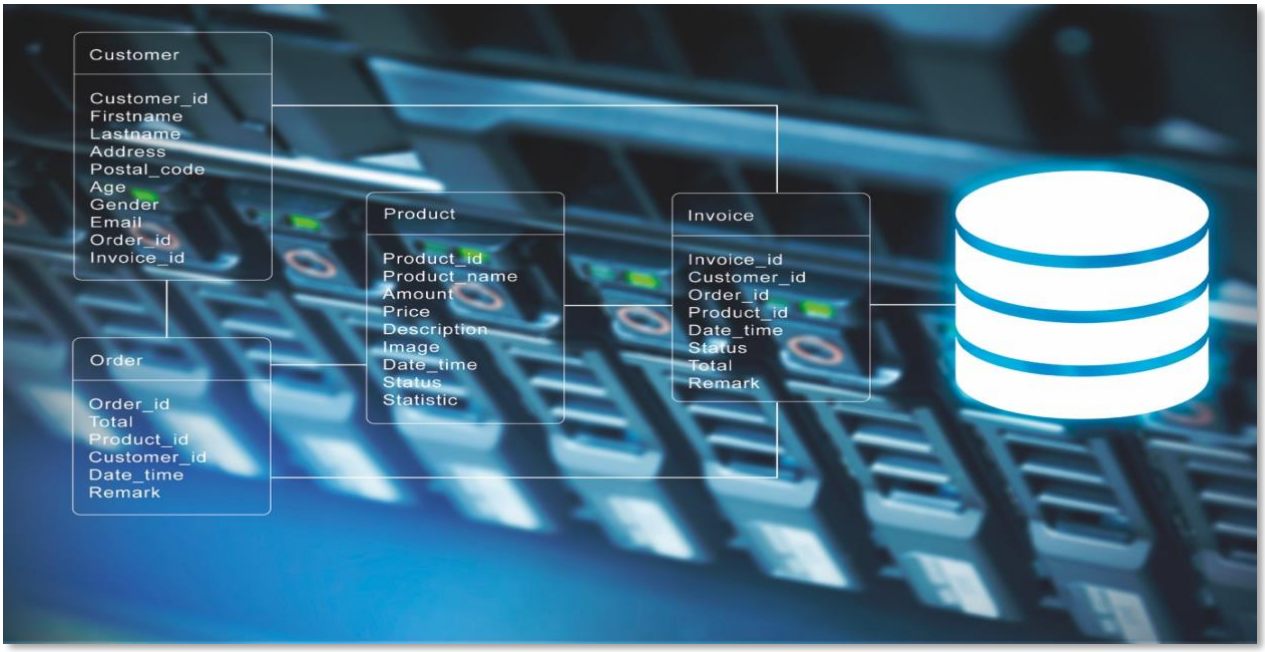
[23] Artikel 28-29 : Overweging 79 en 81

Wanneer een **opdracht** wordt toegewezen, is het belangrijk de nodige contractuele afspraken te maken rond dataprivacy. De aangewezen vorm hiervoor is een Verwerkersovereenkomst. Dit kan een bijlage zijn bij een contract of een samenwerkingsovereenkomst. De afspraken kunnen uiteraard ook verwerkt worden in algemene voorwaarden. Als je al langer met een onderaannemer samenwerkt, moet je er evengoed voor zorgen dat de GDPR wordt nageleefd. Omdat de wetgeving vroeger verschilde en minder klemtoon legde op de verplichtingen voor de verwerker, is een aangepaste versie aangewezen.

In dergelijke verwerkersovereenkomst moeten altijd de volgende clausules opgenomen zijn:

- De rollen van verantwoordelijke en verwerker worden toegewezen aan respectievelijk de opdrachtgever en de uitvoerder / leverancier / onderaannemer.
- De verwerker mag de gegevens enkel gebruiken conform de formele instructies van de verantwoordelijke. Die instructies zet je best op papier.
- De verwerker respecteert de vertrouwelijkheid van de data en legt deze verplichting ook op aan al zijn tijdelijke of vaste medewerkers.
- De verwerker moet een adequate beveiliging van de data opzetten en ervoor zorgen dat ze beschikbaar zijn en blijven voor de opdracht (via back-ups en maatregelen voor continuïteit).
- In geval van een datalek moet de verantwoordelijke onmiddellijk verwittigd worden en moet er een procedure zijn om de impact van het lek in te perken. De verwerker mag nooit zelf de Belgische gegevensbeschermingsautoriteit of de betrokkenen inlichten.
- De verwerker moet de data na het verstrijken van de opdracht (of de overeengekomen bewaartijd) permanent verwijderen en hij moet dit kunnen bewijzen. Indien van toepassing moet hij ze ook aan de opdrachtgever terugbezorgen.
- Data mogen enkel doorgegeven worden aan derden met toestemming van de opdrachtgever. Als de verwerker zelf nog een onderaannemer inschakelt, moet hij afdwingen dat deze dezelfde verplichtingen op zich neemt als vermeld in de overeenkomst.
- De verwerker staat de opdrachtgever toe controle uit te oefenen op de correcte uitvoering door assessments of audits.

Als kleinere organisatie kun je wellicht mee profiteren van het werk van je grotere leveranciers, die zelf vermoedelijk al een verwerkersovereenkomst hebben opgesteld en deze aan hun klanten voorleggen. Binnen onze eigen firma hebben wij er in elk geval voor gezorgd dat onze klanten niet allemaal zelf de inspanning moeten leveren om uit te zoeken wat de rechten en plichten zijn van opdrachtgever en verwerker.



Wij hebben geprobeerd om een evenwichtige overeenkomst op te stellen en bieden die tijdig aan onze klanten aan. Wij engageren ons als verwerker om de GDPR steeds ten volle toe te passen.

Ten slotte moet de verantwoordelijke nagaan of de overeenkomst door de verwerker correct wordt uitgevoerd. Bij een langer lopende overeenkomst zal hij op regelmatige basis moeten **controleren** of dit het geval is. Daarom is het belangrijk dat hij het recht op audit in de contractuele afspraken opneemt. Dit wil natuurlijk nog niet zeggen dat een verantwoordelijke elke onderaannemer elk jaar daadwerkelijk zelf moet gaan auditen.

Grote organisaties doen dit – vaak tot ongenoegen van hun leveranciers – bij de verwerkers die volgens hen een hoog risico lopen om inbreuken te veroorzaken of bij wie een inbreuk grote impact zou hebben. In veel gevallen volstaat het te controleren of de certificatie die de leverancier behaald heeft, jaarlijks hernieuwd wordt. Of je kan de leverancier een vragenlijst laten invullen en ondertekenen waarin hij de genomen maatregelen opsomt. Zoals met alle aspecten van deze wetgeving geldt ook hier dat de te nemen acties moeten worden afgewogen tegenover de kans op een incident en de impact die dit zou hebben.

7. Datalekken

7.1 Incident management

In de vorige hoofdstukken hebben we stapsgewijs besproken hoe je gepaste maatregelen kunt nemen om de persoonsgegevens die je verwerkt, goed te beveiligen. Je moet inzicht hebben in de mogelijke risico's. Daarnaast moet je diverse maatregelen nemen om de risico's als het kan weg te werken of te beperken. Ten slotte moet je ervoor zorgen dat de onderaannemers die je inschakelt zich even goed organiseren als je dat zelf doet. Toch kan er nog altijd iets misgaan. Wat er dan moet gebeuren, is het onderwerp van dit hoofdstuk.

De term datalek[24], of in het Engels 'data breach', wordt gebruikt voor de situatie waarbij vertrouwelijke gegevens verloren gaan of onterecht gewijzigd worden, publiek gemaakt worden of in verkeerde handen terechtkomen. De GDPR schrijft voor dat de verantwoordelijke voor de verwerking van persoonsgegevens zonder onnodig uitstel aangifte doet van datalekken die mogelijk een inbreuk op de privacy van de betrokkenen kunnen vormen. Indien er een ernstig risico is op schade, moeten de betrokkenen zelf ook op de hoogte gebracht worden.

[24] Artikel 4.12; Artikel 33-34 : Overweging 75 en 87-88

Vooraleer we ons mengen in de discussie wanneer je nu wel of niet een datalek moet melden aan de Belgische gegevensbeschermingsautoriteit of de Nederlandse Autoriteit Persoonsgegevens, zouden we eerst willen focussen op het incident management zelf.

De allereerste verplichting die je als verantwoordelijke en als verwerker hebt, is immers incidenten voorkomen en als ze toch voorvallen de impact ervan zoveel mogelijk beperken.

De eerste bekommernis is **incidenten zo vroeg mogelijk opmerken**. Hiertoe kunnen diverse netwerktools worden ingezet, die abnormaal gedrag op het netwerk aan het licht brengen, virussen of malware detecteren of content filtering toepassen. Maar even goed kunnen alerte medewerkers inbreuken opmerken en signaleren. Daarom is het erg belangrijk regelmatig opleidingen voor het personeel te organiseren of bewustmakingsacties op te zetten, zodat het voor iedereen duidelijk is wanneer een situatie abnormaal of verontrustend is. Het is ook belangrijk dat alle medewerkers goed weten wie bij een incident moet ingeschakeld worden.

In tweede instantie moet je dan zo snel mogelijk actie ondernemen om **het incident te stoppen of de impact te beperken**. Alle medewerkers moeten een aantal regels in acht nemen. Als ze informatie aantreffen op een plaats waar deze niet thuishoort, verwijderen ze deze of verwittigen een verantwoordelijke. Dit gaat niet alleen om fysieke dragers, maar ook om bestanden op het netwerk. Als ze vreemden in een beveiligde zone tegenkomen zonder begeleiding, slaan ze alarm. Als alarmen opduiken die wijzen op hacking of infectie van systemen, zullen de systeembeheerders dat systeem zo snel mogelijk onderzoeken en indien nodig preventief uitschakelen.

Bij twijfel is het aangewezen een verwerking stop te zetten of het transport van verwerkte gegevens tegen te houden, totdat duidelijk is of er effectief een probleem is en in hoeverre de verwerkte gegevens nog correct zijn. Op deze manier kan vaak voorkomen worden dat een incident uiteindelijk tot een datalek leidt. Zolang verkeerdelijk verwerkte gegevens niet verspreid of openbaar gemaakt worden, is er nog geen inbreuk gepleegd en is er dus nog geen impact. Strikt gezien is er in dat geval nog geen datalek.

Daarna, eventueel parallel daarmee, kan een **analyse** starten van de feiten. Enerzijds wordt daarmee de eigenlijke **oorzaak van het probleem** vastgesteld. Dan kan je nadenken over **verbeteringen** in de organisatie, in systemen of toepassingen en in de werkwijze van medewerkers, om herhaling te voorkomen.

Anderzijds wordt **de werkelijke of mogelijke impact** van het incident bekeken. Zijn er gevaren voor de vertrouwelijkheid en de integriteit van de data? Zijn de data (deels) persoonsgegevens? Welke gevolgen kan de inbreuk hebben? In veel gevallen zal het wat tijd vergen om te achterhalen hoeveel data impact ondervonden hebben van het incident en hoeveel personen dus betrokken zijn. Het zal ook niet altijd meteen duidelijk zijn of er werkelijk een risico op impact is en al zeker niet hoe groot de schade zou kunnen zijn.

Pas als die vragen beantwoord zijn, kan je beslissen of het noodzakelijk is om het datalek te **melden** aan de gegevensbeschermingsautoriteit of de betrokkenen. Of en wanneer dit moet gebeuren, bespreken we in het volgende hoofdstuk.

Los daarvan moet je elk incident **intern in een register noteren**. Of er nu een echte inbreuk plaatsvindt of het eerder om een 'bijna-botsing' gaat, het incident moet altijd geanalyseerd worden.

Die informatie is belangrijk om de bestaande procedures en richtlijnen te evalueren en na te gaan of de genomen maatregelen afdoende bescherming bieden tegen de mogelijke risico's. Je moet de oorzaken van een incident bijhouden en de voorgenomen verbeteracties opsommen. Door dit systematisch op te volgen, verbeter je stelselmatig de beveiliging van je organisatie.

In extreme gevallen kan een datalek ook leiden tot een regelrechte ramp. Een organisatie kan met immense communicatieproblemen geconfronteerd worden als zeer gevoelige informatie gelekt is over een zeer groot aantal betrokkenen. Soms gebeurt het dat het lek buiten de eigen organisatie bekend geraakt is en dat de pers al op de hoogte is. Dan is het goed te kunnen terugvallen op voorbereide scenario's voor **crisiscommunicatie**. Als je organisatie een verzekering voor cybersecurity heeft afgesloten, kan de verzekeringsmaatschappij hierbij soms hulp bieden.

Als het vermoeden bestaat dat er criminele feiten gepleegd zijn, moet je er ook voor zorgen tijdig een **juridisch dossier** op te bouwen. Soms is het van belang snel een back-up te maken van de situatie op het ogenblik dat het incident ontdekt werd of logfiles opzij te zetten, voordat deze informatie verdwijnt of gewijzigd raakt door stappen in het oplossingsproces van het incident. Het is duidelijk dat een dergelijke stap soms zal indruisen tegen wat nodig is om snel het bestaande probleem op te lossen. Als politie of gerecht in het spel zijn, moet je heel goed opletten wat je wel of niet eigenmachtig kan doen, zeker als je de rol van verwerker hebt. Schakel alvast zo snel mogelijk de verantwoordelijke in.

Zelfs als de overheden je verplichten informatie af te staan, blijft het jouw verantwoordelijkheid om deze informatie maximaal te beschermen en moet je erover waken geen gegevens, bijvoorbeeld van andere betrokkenen, bloot te stellen indien dit voor het onderzoek niet nodig is.

Het is verstandig deze achtereenvolgende stappen goed te documenteren, zodat iedereen in de organisatie ze kent en ernaar handelt. Dit is ook nuttig om aan te tonen dat je de verplichtingen van de GDPR ernstig neemt.

7.2 Meldingsplicht

Bij het vaststellen van een datalek is de eerste bekommernis de impact minimaal te houden. Daarover hadden we het in het vorige hoofdstuk. Los daarvan vereist de GDPR dat je als verantwoordelijke voor de verwerking zonder onredelijke vertraging bij de Belgische gegevensbeschermingsautoriteit of Nederlandse Autoriteit Persoonsgegevens melding[25] maakt van elk datalek dat waarschijnlijk een risico op een inbreuk tegen de privacy inhoudt. Als het risico waarschijnlijk hoog is, moeten de betrokkenen zelf ook op de hoogte gebracht worden.

Deze verplichting roept heel wat vragen op. Wanneer is een informatiebeveiligingsincident ook effectief een datalek? Wanneer vormt een datalek een risico op inbreuk op de privacy? Wanneer is er ernstig risico op schade? Vanaf welk ogenblik ben je op de hoogte en loopt de tijd die je hebt om aangifte te doen?

Als er persoonsgegevens bij het incident betrokken zijn, verwittig dan standaard je Data Protection Officer. Als er geen officiële DPO is, moet in elk geval iemand deze rol op zich nemen. Het is de DPO die het best kan bepalen welk gewicht de data hebben en hoe groot de impact van een inbreuk zou kunnen zijn voor de betrokkenen en voor de verantwoordelijke voor de verwerking (je eigen organisatie of misschien je klant, als je zelf verwerker bent in opdracht van een ander). De DPO adviseert de organisatie over de communicatie die moet gebeuren. Hij is het best geplaatst om te beslissen of een aangifte bij de Belgische gegevensbeschermingsautoriteit nodig is en welke informatie al meteen kan doorgegeven worden.

Tip:

Aan de hand van deze drie vragen kan je eenvoudig uitmaken of aangifte nodig is:

1. Zijn er effectief data gelekt? Als een incident het risico op een lek inhield, maar in feite zijn geen data openbaar geworden of bij verkeerde personen terechtgekomen, blijft het bij een incident. Dit noteer je wel in je interne incidentenlijst maar aangifte is niet nodig.

[25] Artikel 33 en 34 : Overweging 85-88

2 Is er waarschijnlijk geen risico? Als data buiten de beveiligde zones of buiten je organisatie terechtgekomen zijn, is het nog steeds mogelijk dat er dankzij de beschermingsmaatregelen eigenlijk geen risico is. De data kunnen bijvoorbeeld degelijk geëncrypteerd zijn en zullen dus door buitenstaanders niet gebruikt kunnen worden.
3 Is het onmiddellijke risico op schade voor de betrokkenen groot? Bij een datalek met betaalkaartgegevens is er kans op financiële schade en moeten de betrokkenen zo snel mogelijk verwittigd worden, zodat ze zelf maatregelen kunnen nemen. Dit kan ook het geval zijn als het gaat om diverse soorten gevoelige informatie. Gaat het om triviale data, dan is het zeker minder dringend iedereen op de hoogte te brengen.

De GDPR heeft ook begrip voor situaties waarin het bijna onmogelijk is alle betrokkenen individueel in te lichten. Een publieke communicatie voldoet dan ook.

De GDPR legt ook vast welke informatie de melding moet bevatten:

- Een omschrijving van de inbreuk, met zo mogelijk de vermelding van het type van betrokkenen en de categorieën van gegevens.
- Indien mogelijk bij benadering het aantal betrokkenen.
- De contactgegevens van de DPO of het contactpunt voor dataprivacy.
- De waarschijnlijke gevolgen van de inbreuk.
- De door het incidentteam genomen maatregelen om de impact te beperken.

Gedeelten van deze informatie zijn wellicht niet onmiddellijk bekend en kunnen pas na verdere analyse vastgesteld worden. De GDPR zegt dan ook niet dat 'onmiddellijk' aangifte gedaan moet worden maar wel 'zonder onnodig uitstel'. Binnen de 72 uur nadat het datalek bij de verantwoordelijke is vastgesteld, geldt als de norm. Mits een goede motivatie kan de melding nog uitgesteld worden. De informatie over de inbreuk kan overigens na de eerste aangifte later aangevuld worden.

Als je niet de verantwoordelijke bent, maar als verwerker in opdracht optreedt, moet je bij datalekken extra op je hoede zijn. Je loopt immers het risico je eigen verantwoordelijkheidsdomein te overschrijden en daardoor zelf een grotere aansprakelijkheid te krijgen.

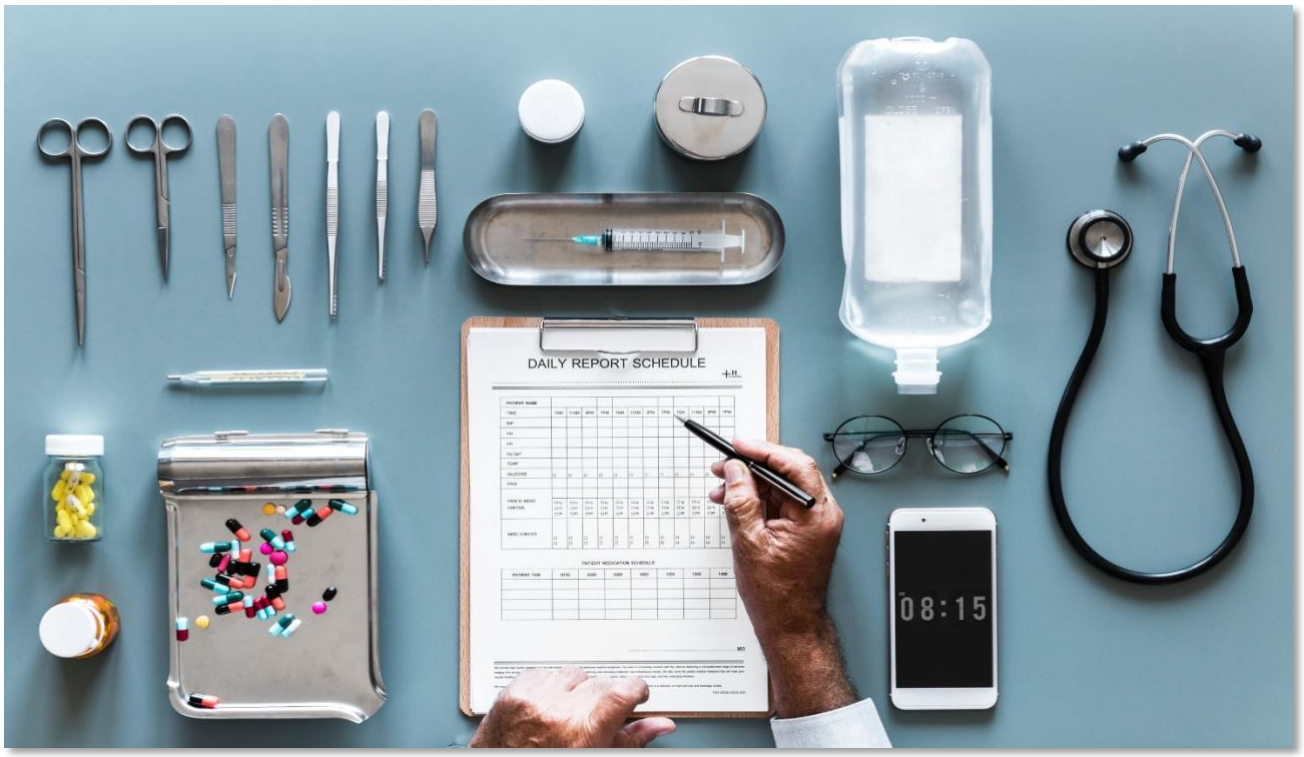
In de meeste verwerkersovereenkomsten wordt daarom duidelijk vastgelegd dat een verwerker die een datalek vaststelt, onmiddellijk de verantwoordelijke moet contacteren en nooit zelf mag communiceren met de Belgische gegevensbeschermingsautoriteit of met de betrokkenen. Communiceren met de pers kan je eveneens beter overlaten aan de verantwoordelijke.

Waar de verantwoordelijke van de wetgever in normale omstandigheden tot 72 uur de tijd krijgt voor zijn melding, is de verwachting dat een verwerker die een inbreuk vaststelt, dit wel zo snel mogelijk doorgeeft aan de verantwoordelijke. Dat geeft die laatste de gelegenheid meteen zijn taken op zich te nemen. Contracten leggen de verwerker vaak op om binnen de 24 uur te reageren, hoewel de wet zelf eveneens van 72 uur spreekt.

Het zal niet altijd gemakkelijk zijn om te bepalen welke communicatie en welke meldingen noodzakelijk zijn. Een datalek niet melden is een strafbaar feit en stelt de verantwoordelijke bloot aan potentieel erg hoge boetes. Anderzijds is het overzicht van meldingen van datalekken publieke informatie. Geen enkele firma staat daarin graag vermeld en al zeker niet als achteraf zou blijken dat er niet echt sprake was van een datalek of dat de data zo goed beschermd waren dat er geen enkel risico op schade is geweest. Voordat dit duidelijk is, kan je al een hoop imagoschade opgelopen hebben. Omgekeerd wil ook niemand de reputatie hebben dat hij ernstige problemen heeft willen verdoezelen. In dat opzicht is openheid en transparantie altijd te verkiezen.

We mogen wellicht nog richtlijnen verwachten van de autoriteiten om beter af te bakenen in welke gevallen een aangifte wel of niet aangewezen is. Privacy specialisten waarschuwen overigens ook voor het gevaar dat bedrijven te snel aangifte zullen doen om boetes te voorkomen en dat de autoriteiten daardoor overspoeld zullen worden door aangiftes die ze niet kunnen controleren en verwerken. Dat is bijvoorbeeld in Nederland, waar deze meldingsplicht al een tijd geldt door een nationale wet, aanvankelijk gebeurd.

Ons advies is om in elk geval ieder incident te noteren in de interne incidentenlijst, die eveneens een verplichting van de GDPR is. Daarin vermeld je de vastgestelde feiten, de gevolgen en de genomen corrigerende maatregelen. Als je betrokkenen niet inlicht of geen aangifte doet, kan je je argumentatie daar bewaren. Zo kan je later altijd aantonen dat een incident wel degelijk was opgemerkt en dat je adequate maatregelen nam. Overigens levert dergelijke opvolging ook een belangrijke bijdrage aan de verbetering van je procedures en beschermingsmaatregelen.



8. Rechten van de betrokkene

8.1 Recht op informatie

In deze publicatie hebben we tot hiertoe voornamelijk gesproken over de verplichtingen die de GDPR met zich meebrengt voor bedrijven of organisaties die persoonsgegevens verwerken. We hebben de wet vooral bekeken vanuit het standpunt van de verantwoordelijke voor gegevensverwerking en de verwerker. Het wordt tijd dat we de focus even verleggen naar de betrokkene zelf.

Een hoofdbedoeling van de GDPR is immers de rechten als individueel persoon[26] vast te leggen voor de vele gegevens die over jou circuleren en die door anderen gebruikt worden. Je kunt als betrokkene wel degelijk greep houden op deze informatie, ook al zijn je rechten niet absoluut.

Eén van de belangrijkste woorden in de GDPR is **transparantie**. Een dataverwerker moet tegenover de betrokkenen van wie hij de data verwerkt, openheid nastreven. Het moet gemakkelijk zijn om te weten te komen welke gegevens een verwerker over je bewaart en verwerkt, wat hij met deze gegevens doet en waarvoor deze verwerkingen nodig zijn. Hij moet je dat in eenvoudige, duidelijke taal kunnen uitleggen. In hoofdstuk 5 hebben we reeds uitvoerig behandeld hoe een firma of organisatie bijvoorbeeld op hun website deze informatie kan aanleveren in de vorm van **een privacyverklaring**.

Vooral wanneer een verwerker gegevens van je vraagt met de bedoeling deze op te slaan en te gaan gebruiken, moet hij je **vooraf** goed inlichten over zijn bedoelingen, de mogelijke gevolgen en de risico's die je loopt. Hij moet je duidelijk maken dat ook voor jou de voordelen opwegen tegen de nadelen.

Daarenboven moet de verantwoordelijke voor de verwerking aangeven **wat je kunt doen in geval van vragen of bij klachten**. Je moet een direct aanspreekpunt krijgen binnen de organisatie.

De verwerker moet je erop wijzen dat je tegen de verwerking een klacht kunt indienen bij de Belgische gegevensbeschermingsautoriteit of in Nederland de Autoriteit Persoonsgegevens. Maar daar heb je uiteraard wel een gegronde reden voor nodig.

[26] Artikel 12-15; Artikel 23 : Overweging 58-64

Naast het recht op algemene informatie heb je als individuele betrokkene ook specifieke rechten wat betreft je eigen persoonlijke gegevens. Iedereen kan zich tot een verantwoordelijke voor verwerking richten **om inzage te krijgen in de gegevens die deze firma of organisatie over hem bewaart en in de verwerkingen die met die gegevens gebeuren**. Dit lijkt misschien een eenvoudig verzoek, maar het kan een organisatie heel wat werk bezorgen. Correct reageren op dergelijke vragen, vergt een goede voorbereiding en een duidelijke procedure, temeer omdat de betrokkenen volgens de GDPR binnen een maand antwoord moeten krijgen. Ofwel moet de verantwoordelijke tegen dan de gevraagde informatie bezorgen ofwel moet hij op zijn minst een plausibele verklaring geven waarom hij meer tijd nodig heeft.

Er zijn een aantal belangrijke struikelblokken voor het vervullen van deze verplichting. In de eerste plaats moet de verantwoordelijke goed weten welke informatie waar te vinden is. Voor bestanden met contactgegevens in een CRM-toepassing of voor personeelsgegevens in een administratief systeem is dat niet zo moeilijk.

Maar veel informatie zit verspreid over zogenaamde niet-gestructureerde informatie, in papieren dossiers, in bestanden die niet via document management beheerd worden of ergens lokaal bij individuele werknemers. Die gegevens zijn veel minder gemakkelijk bij elkaar te krijgen. De GDPR zegt bovendien expliciet dat deze dienstverlening gratis moet zijn, behalve als de verzoeken manifest ongefundeerd of overdreven zijn.

Anderzijds komt dit **recht op inzage ook in conflict met andere rechten en belangen**. De verantwoordelijke moet er bijvoorbeeld voor opletten dat hij door informatie aan een betrokkene door te geven niet tegelijk de rechten van een andere betrokkene schendt. Als een individu bijvoorbeeld inzage wil krijgen in alle documenten of mails waarin hij of zij vernoemd wordt, zal een organisatie daar eigenlijk zelden of nooit zonder meer op kunnen ingaan. Deze documenten bevatten immers tegelijk informatie van andere betrokkenen en ook hun privacy moet beschermd worden. Sommige informatiebronnen bevatten overigens ook andere vertrouwelijke gegevens, waarvan het ontsluiten de belangen van de firma kunnen schaden. In al deze gevallen is het nodig verschillende rechten tegen elkaar af te wegen en tot een evenwichtig standpunt te komen.

Op die manier kan het zijn dat een verzoek van een betrokkene niet kan ingewilligd worden. Als aanvrager moet je dan wel een toelichting krijgen waarom de verwerker niet op je vraag kan ingaan.

Behalve het recht op informatie geeft de GDPR de betrokkene nog heel wat meer rechten. Die bespreken we in het volgende hoofdstuk.

8.2 Rechten op de eigen gegevens

In het vorige hoofdstuk bespraken we het recht op informatie van de betrokkenen. Elke verantwoordelijke voor gegevensverwerking moet transparant zijn over het type van data die hij bijhoudt, de verwerkingen die ermee gebeuren en het doel daarvan. Daarnaast beschikt elke betrokkene over het recht om zijn eigen individuele gegevens op te vragen.

De rechten van de betrokkene (en dus ook de verplichtingen voor een verantwoordelijke) gaan echter nog een heel eind verder. Een betrokkene kan ook **vragen om gegevens die je over hem bewaart en verwerkt te corrigeren, aan te vullen of zelfs te wissen**[27]. Ook in dit geval gaat het niet om een absoluut recht en moeten de mogelijkheden om aan het verzoek te voldoen afgewogen worden tegenover andere rechten of wettelijke verplichtingen. Gegevens die van overheidswege gedurende een bepaalde tijd gearchiveerd moeten worden, kunnen uiteraard niet op verzoek van één individu verwijderd worden. Gegevens moeten soms een tijdlang bijgehouden worden om aan alle contractuele verplichtingen te voldoen.

[27] Artikel 16-23 : Overweging 65-73

Een verwerker moet zelfs een beperkt aantal gegevens bijhouden om te documenteren dat hij voldaan heeft aan de aanvraag van een betrokkene om zijn gegevens te wissen.

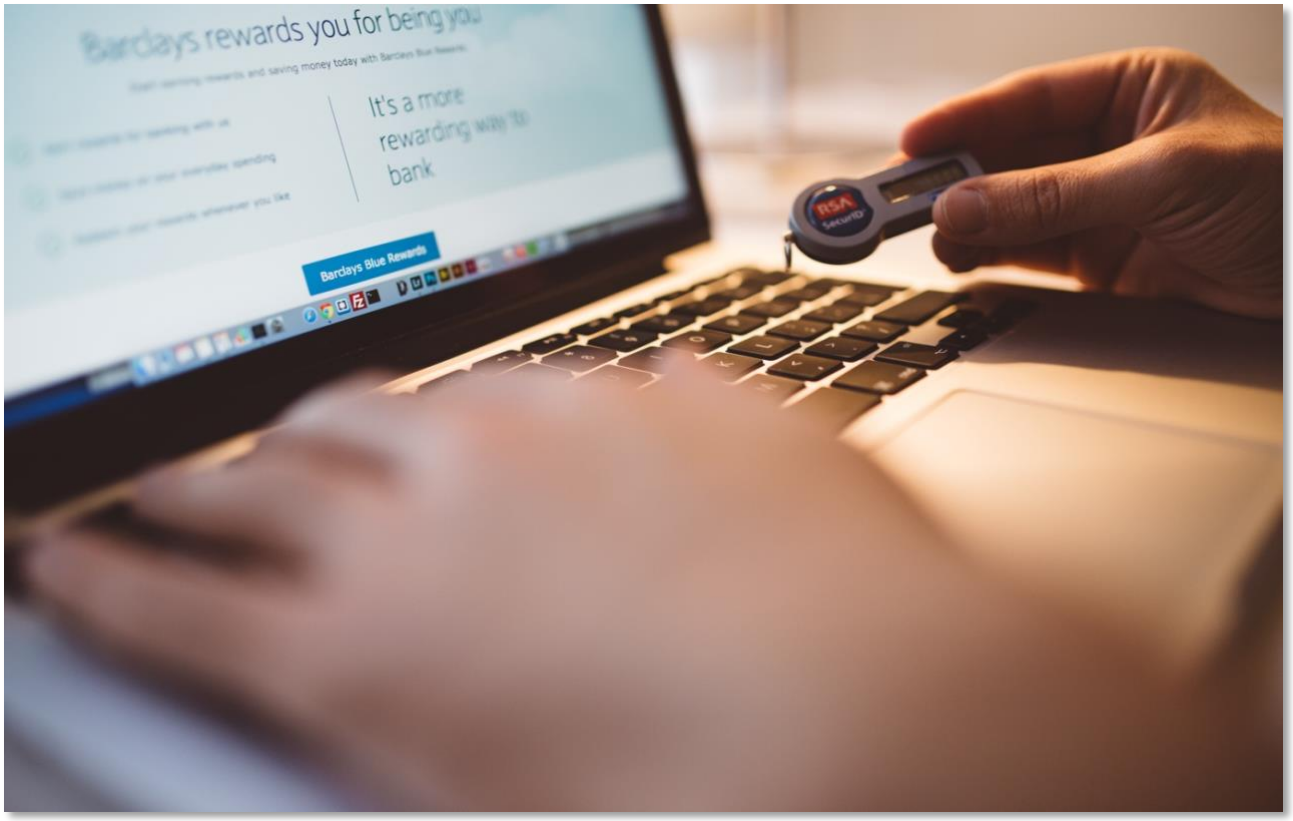
Ook het recht om te corrigeren is vanzelfsprekend relatief. Een vastgelegd verslag van een evaluatie kan op vraag van een werknemer niet zonder meer gewijzigd worden, maar hij kan zijn rechten uitoefenen door er een commentaar aan toe te voegen. Correcties of aanvullingen zijn logisch – zelfs nuttig – als de gegevens bijvoorbeeld via derden verkregen zijn. Het wordt echter juridisch een stuk moeilijker als het gaat om verrijkingen die door de verantwoordelijke zelf zijn doorgevoerd en voor hem een toegevoegde waarde zijn.

In regel geldt dat dergelijke verzoeken om aanpassingen aan data ook gelden voor alle derden aan wie deze data waren doorgegeven (bijvoorbeeld partners of onderaannemers). De verantwoordelijke moet ervoor instaan dit zo goed als mogelijk door te trekken. Rond dit fameuze 'recht om vergeten te worden' zijn reeds een paar geruchtmakende processen gevoerd bij sociale media. Het zal duidelijk zijn dat het absoluut niet eenvoudig is om verzoeken zo ver door te voeren. Dit is een belangrijk argument voor een verantwoordelijke om in overeenkomsten met onderaannemers te laten opnemen dat gegevens na verwerking onmiddellijk verwijderd moeten worden.

Verder kan een betrokkene **vragen om de verdere verwerking van zijn gegevens stop te zetten of op te schorten,** terwijl de data toch bewaard blijven. Dit kan de aangewezen werkwijze zijn bij een lopende klacht waarover nog geen uitspraak is gedaan door de autoriteiten, bijvoorbeeld als de betrokkene de rechtmatigheid van de verwerking betwist. Dergelijk verzoek kan natuurlijk niet ingewilligd worden als de verwerking berust op een wettelijke verplichting of in het kader van een overheidstaak. Zoals we eerder al bespraken, kan een verwerking die gebeurde op grond van de toestemming van de betrokkene, altijd worden stopgezet door deze **goedkeuring in te trekken**. In dat geval is de verantwoordelijke ook verplicht de data te verwijderen.

Ten slotte beschikt de betrokkene over **het recht op 'data portabiliteit'**. Dit is een regeling die eerder in de privacywetgeving was opgenomen en verplichtingen oplegde aan verleners van elektronische diensten. De achterliggende bedoeling was om te voorkomen dat dienstverleners hun klanten zouden 'gijzelen' doordat ze over al hun gegevens beschikken en deze verloren zouden gaan als de gebruiker van dienstverlener zou willen veranderen. Niemand wil natuurlijk al zijn online bewaarde foto's, blogs of mails kwijtraken. Dit recht van de betrokkene is nu ook in de GDPR opgenomen en is van toepassing op alle verwerkingen van persoonsgegevens.

In deze veel ruimere context is die overdraagbaarheid vaak niet praktisch. Bovendien zorgt het ook voor conflicten met andere rechten. Een verantwoordelijke die complexe bewerkingen met data heeft gedaan (waaraan soms logaritmen ten grondslag kunnen liggen die het intellectuele eigendom van de firma zijn), wenst die resultaten niet zomaar prijs te geven. De meest gevolgde interpretatie is dan ook dat het recht op data portabiliteit eigenlijk enkel geldt voor gegevens die de betrokkene eerst zelf ter beschikking van de verwerker heeft gesteld.



Tip:

Hoe de afhandeling van al deze verzoeken moet gebeuren, zou elke organisatie best in een goede procedure vastleggen.

- Om te beginnen is het nodig om aan de betrokkenen duidelijk te maken wie ze moeten aanspreken met hun vragen en wie in een organisatie hiervoor verantwoordelijk is. Dat kan bijvoorbeeld opgenomen worden in een privacyverklaring.
- Binnen de organisatie moeten verzoeken snel aan de juiste persoon doorgegeven worden voor verdere verwerking – iedereen moet op de hoogte zijn van de procedure.
- Er moet een duidelijk omschreven methode zijn om vast te stellen of de identiteit van de aanvrager overeenkomt met die van de betrokkene wiens data worden opgevraagd. Meestal wordt gesuggereerd dat men de aanvrager om een kopie van zijn identiteitskaart vraagt.
- Er moeten ook regels zijn die bepalen welke informatie mag gegeven worden en welke eventueel niet, omdat ze bijvoorbeeld ook vertrouwelijke gegevens kan bevatten over andere personen of bedrijfsgeheimen. De te volgen argumentatie moet gedocumenteerd zijn. Hierbij moet je evenwichtig met ieders recht omgaan – ook de rechten van de betrokkene zijn niet absoluut.
- Een opvolgingssysteem moet ervoor zorgen dat alle aanvragen tijdig behandeld worden en dat documentatie over de voortgang en de genomen beslissingen wordt bijgehouden.

Het is duidelijk dat de uitoefening van deze rechten voor praktische problemen zal zorgen bij de verwerkers van data. Sommigen vrezen dat de wet zal gebruikt worden door zogenaamde dataprivacy-activisten om bepaalde door hen geviseerde bedrijven te bestoken met massaal georganiseerde aanvragen. Maar de GDPR biedt hiertegen wel enige bescherming door aan te geven dat de aanvragen gemotiveerd moeten worden en niet excessief mogen zijn (bijvoorbeeld door ze telkens te herhalen). Op voorwaarde dat de verantwoordelijke dit kan aantonen, is hij niet verplicht op dergelijke verzoeken in te gaan. Omgekeerd is het uiteraard toe te juichen dat wij als individu dankzij de GDPR in zekere mate meester blijven over de gegevens over onze eigen persoon en dat bedrijven en organisaties een kader hebben om respectvol en zorgvuldig met persoonsgegevens om te gaan.

9. Aansprakelijkheid onder de GDPR

Nu we zo ongeveer het hele terrein van de GDPR overlopen hebben, blijven er nog een paar onderwerpen over die we meer globaal moeten behandelen. Eén ervan is de accountability of aansprakelijkheid[28] van verwerkers en zeker van verantwoordelijken voor de verwerking. Iedereen die persoonsgegevens verwerkt, is verplicht de voorschriften van de GDPR na te komen en moet op elk moment ook duidelijk kunnen bewijzen dat hij dit doet. Wie vertrouwd is met audits, weet wat dit betekent. Na de vraag hoe je je georganiseerd hebt om aan bepaalde verplichtingen te voldoen, volgt steevast ook de opdracht aan te tonen dat je daadwerkelijk je procedures volgt en hierop voldoende controle uitoefent bij je medewerkers. Daarover gaat dit hoofdstuk.

Om te kunnen bewijzen dat je alle aspecten van de GDPR kent en begrijpt en je die hebt doorgetrokken in je eigen organisatie, is er wel wat administratie nodig. Vooral in een kleine firma, organisatie of vereniging komt het erop aan dit pragmatisch, maar toch volledig door te voeren. We hebben hier en daar al wat tips gegeven hoe je hieraan kunt voldoen. Het zal er in de toekomst op aankomen de documentatie steeds op peil te houden.

Om te beginnen moet je **voldoende kennis in huis** halen. Organisaties met een Data Protection Officer vertrouwen de verantwoordelijkheid hiervoor aan hem (en zijn medewerkers) toe. Maar ook zonder DPO moet je geïnformeerd zijn en je werknemers opleiden.

Het centrale punt om je compliance aan te tonen is **het register van verwerkingen van persoonsgegevens**. Het is op zichzelf al een vereiste van de GDPR dergelijk register bij te houden. Tegelijk is dit het ideale vertrekpunt om je beheersing van dataprivacy te documenteren. Voor elke beschreven verwerking toon je hierin aan dat je hebt nagedacht over het doel en de rechtsgrond voor de verwerking. Je bewijst zo ook dat je de risico's op een datalek hebt afgewogen en daartegen maximale beveiliging hebt georganiseerd. Uiteraard moet je ook een goede procedure uitwerken om te verzekeren dat deze informatie compleet blijft. Elke verwerking die erbij komt, moet in het register opgenomen worden. Hier is een belangrijke rol weggelegd voor de Data Protection Officer, die hierbij helpt en toezicht houdt op het stipte uitvoeren van deze procedure.

[28] Artikel 5.2; Artikel 24 : Overweging 74

Voor belangrijke projecten kan dit vooronderzoek verder geformaliseerd worden.

Dan spreken we van een 'dataprivacy impact analyse' (DPIA). Dit is een formele doorlichting van een verwerking met de bedoeling alle mogelijke risico's voor inbreuken op de privacy te definiëren en alle beschermende maatregelen op te sommen. Zo kan je afwegen of de doelstelling en de rechtsgrond voor de verwerking wel degelijk opwegen tegen de risico's die nog overblijven. Voor intensieve verwerkingen van speciale categorieën van persoonsgegevens moet dergelijke DPIA ter goedkeuring voorgelegd worden aan de Belgische gegevensbeschermingsautoriteit).

Alle **beveiligingsmaatregelen** moeten uiteraard goed gedocumenteerd worden. Bij controle veronderstelt men dat je meteen kunt laten zien welke procedures van toepassing zijn, van wanneer de laatste versie dateert, op wie elke procedure van toepassing is en of deze medewerkers op de hoogte zijn en de instructies kennen. Als bij bepaalde procedures terugkerende controleacties horen, is het belangrijk op een of andere manier vast te leggen dat deze controles ook daadwerkelijk gebeuren.

Technische logbestanden of rapporten van monitoring hou je best een tijdlang bij. Indien manuele controles gebeuren, moet je hiervan bijvoorbeeld een kort verslag maken of een lijstje bijhouden, om aan te tonen wie op welk moment deze controles heeft uitgevoerd.

Het hele beveiligingssysteem moet ook minstens één keer per jaar geëvalueerd en bijgestuurd worden, rekening houdend met wijzigingen in de organisatie, in de gebruikte tools en technieken of in de beschikbare beveiligingsoplossingen.

Je moet verder veel zorg besteden aan **het loggen van incidenten en datalekken**. Elk voorval dat indruist tegen de normale beveiligingsprocedures of elke vaststelling die aan het licht brengt dat er een risico op een datalek is of geweest is, moet nauwkeurig genoteerd worden in een incidentenlijst. De items in dergelijke lijst dienen vanzelfsprekend verder onderzocht te worden, om de dieperliggende oorzaak te ontdekken. Tegelijk worden acties gedefinieerd om het risico te verminderen. Dit kan gaan om extra technische beveiligingsmaatregelen of om bijkomende of aangepaste procedures en controles, om nieuwe rapportering of Logging, enz. Om je aansprakelijkheid te kunnen aantonen is het belangrijk dit te documenteren. Daar heb je niet per se een ingewikkeld opvolgingssysteem voor nodig, maar op zijn minst enkele overzichtelijke lijsten: alle incidenten met hun analyse en de afgesproken remediëring, alle actiepunten, de verantwoordelijke ervoor en de status.

Speciale aandacht is nodig voor de **contractuele afspraken met partners of leverancier**s. Aan de hand van een verwerkersovereenkomst moet je afdwingen dat ook je onderaannemers de wetgeving adequaat opvolgen. Het is ook een goed idee een register bij te houden van onderaannemers aan wie je verwerkingen van persoonsgegevens toevertrouwt en goed vast te leggen wat hun opdracht precies is en op welke manier je daarover afspraken maakt. Daar kan je dan de specifieke overeenkomst aan koppelen. Omgekeerd moet je er ook over waken dat je zelf goed in orde bent **als je als verwerker optreedt in opdracht van een klant**. Dergelijke verwerkingen moeten in je register opgenomen zijn, ook al zijn minder details nodig dan voor de verwerkingen waarvan je zelf de verantwoordelijke bent. Ook in dit geval is het belangrijk alle cruciale afspraken in een verwerkersovereenkomst op te nemen.

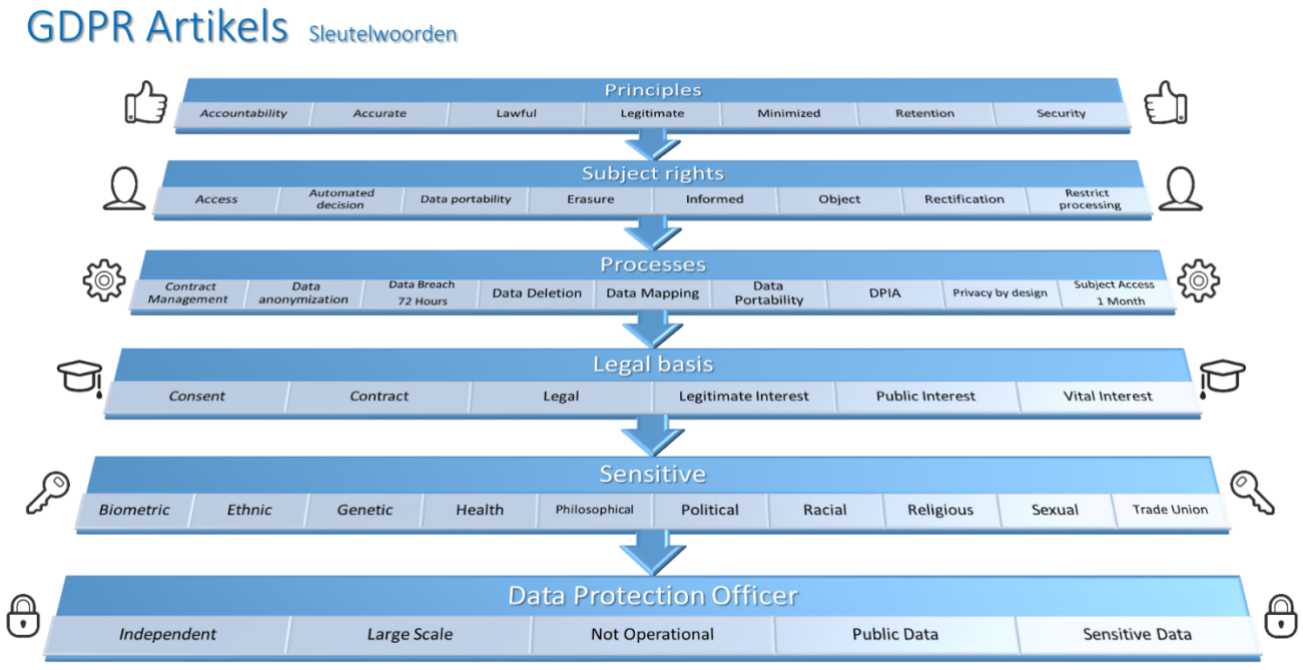
Ten slotte moet je kunnen aantonen dat je **de rechten van de betrokkenen daadwerkelijk garandeert**. Er moeten goede afspraken zijn over de te volgen procedure als een betrokkene vragen stelt. Ook van alle hieraan verbonden activiteiten hou je best een soort van register bij.

Als je elke aanvraag van een individuele persoon noteert, met de datum en tijd dat deze is binnengekomen en vervolgens elke actie die genomen wordt, kun je in eerste instantie voor jezelf opvolgen of je tijdig reageert en de gepaste antwoorden geeft.

Bij een controle door de gegevensbeschermingsautoriteit (GBA of AP) of in geval van een klacht kun je dan altijd aantonen dat je naar je beste vermogen de wet naleeft. Vooral als je aan bepaalde verzoeken niet wilt of kunt voldoen, is het van belang de gevolgde argumentatie bij te houden.

Het is dus niet voldoende wettelijk in orde te zijn. Je moet dit ook documenteren en kunnen bewijzen. Het is belangrijk om bij alle toekomstige projecten steeds te anticiperen op de mogelijke risico's voor dataprivacy. Dat bespreken we in het volgende hoofdstuk.

Voor de liefhebbers hieronder een overzicht van alle kernwoorden die in de 99 artikels over de General Data Protection Regulation voorkomen in hun juiste context.



10. De toekomst – privacy by design

Een mooi onderwerp om onze lange wandeling doorheen het landschap van de dataprivacy af te ronden, is 'gegevensbescherming door ontwerp[29]' (beter bekend als 'privacy by design'). De wetgever wil immers dat alle verwerkers bij hun toekomstige plannen voor het verwerken van persoonsgegevens vanaf het begin rekening houden met het recht op privacy.

De opstellers van de GDPR gaan ervan uit dat we een soort van privacy reflex krijgen. De vereisten van de wetgeving worden dan een natuurlijk en vanzelfsprekend onderdeel van het bouwen van een applicatie, het inrichten van een website, het organiseren van een enquête of het opzetten van wetenschappelijk onderzoek. Als het niet nodig is, kunnen we persoonsgegevens beter niet verzamelen en verwerken. En als er wel een goede reden voor is, moeten we **de verwerkingen beperken tot wat strikt noodzakelijk is**. Bij alle nieuwe initiatieven is dus een denkoefening nodig.

- Tijdens de analyse voor een nieuwe applicatie of bij het ontwerpen van een database was het vroeger misschien aangewezen eerder wat meer attributen of velden aan een bestand toe te voegen ('je weet maar nooit'). Nu komt het er eerder op aan het aantal gegevens zo beperkt mogelijk te houden, gericht op de specifieke doelstelling.
- In een databank kan best meteen opgeslagen worden wanneer een bepaald gegeven verouderd is of achterhaald of gewoonweg niet langer meer bewaard mag worden. Op die manier is het niet moeilijk gegevens systematisch te wissen als we ze niet meer nodig hebben of als we de juistheid ervan niet langer kunnen garanderen.

[29] Artikel 25 : Overweging 78

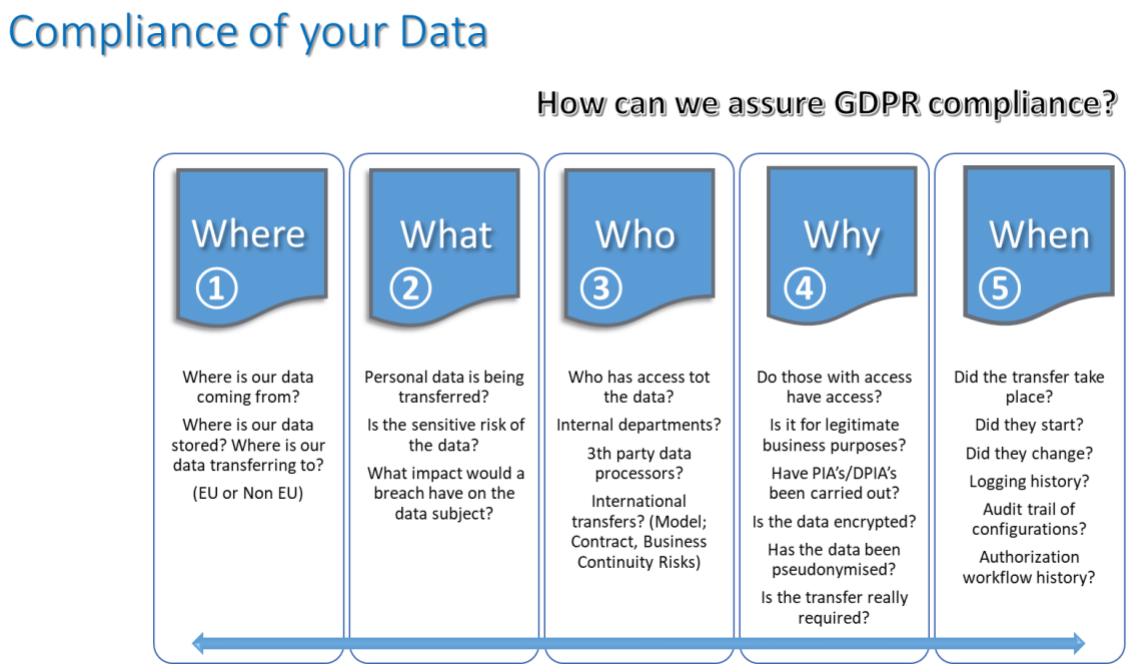
Een toepassing kan in de toekomst ook best meteen functies bevatten om **de rechten van de betrokkenen** te garanderen en de praktische invulling daarvan gemakkelijker te maken.

- Overal waar in een toepassing persoonsgegevens aan betrokkenen gevraagd worden, moet tegelijk informatie beschikbaar zijn over het doel, de duur, de risico's en de beschermingsmaatregelen van de verwerking. Een app voor een smartphone die bijvoorbeeld sportprestaties registreert, moet de betrokkene voor het eerste gebruik voldoende inlichtingen geven over de informatie die op de achtergrond verzameld en opgeslagen wordt en over de bedoelingen van de bouwer van de app. Dit moet handig ingebouwd worden in de userinterface voor apps.
- Op dezelfde manier moet iedereen die op een websitegegevens tracht te vergaren over de bezoekers, tijdig duidelijke achtergrondinformatie verstrekken over de verwerking. Verschillende mogelijke doelstellingen moeten maximaal gescheiden worden.
- Een toepassing kan in de toekomst ook best functies bevatten die de betrokkenen de mogelijkheid geeft hun gegevens op te vragen en, als de situatie dat toelaat, ze te corrigeren, aan te vullen of te wissen. Dit is uiteraard enkel mogelijk als er geen conflicten tussen de rechten van de betrokkene en andere belangen zijn.

Privacy by design houdt ook in dat je bij het ontwerpen van een toepassing meteen nadenkt over **manieren om de gegevens zo goed mogelijk te beschermen**. Zo kan je bijvoorbeeld de toepassing op die manier bouwen dat overal waar mogelijk encryptie wordt gebruikt. Een website kan gebruik maken van encryptie protocollen als https en data-uitwisseling kan gebeuren via geëncrypteerde kanalen en met geëncrypteerde bestanden. Als data na verwerking nog een tijdje bewaard moeten worden, kan dat eveneens in geëncrypteerde vorm gebeuren, bijvoorbeeld in een beveiligd digitaal archief. Al deze maatregelen verminderen het risico dat data publiek gemaakt worden of in verkeerde handen vallen. Als ze vanaf het ontwerp in overweging genomen worden, zijn de kosten veel lager dan wanneer later aanpassingen moeten gebeuren. Een maatregel die je soms kan overwegen, is het pseudonimiseren van gegevens. Dit houdt in dat je de directe verwijzingen naar concrete personen uit de bestanden weghaalt. Daardoor vermindert het risico op inbreuken als er toch iets misloopt met een bestand.

Als laatste item vermelden we nog de term **'privacy by default'**. Hiermee wordt bedoeld dat in alle toepassingen waar de gebruiker ervoor kan kiezen om gegevens al dan niet openbaar te tonen, de standaardinstellingen altijd de meest veilige moeten zijn. Het gaat dan om de keuze om gegevens met anderen te delen, om ze beschikbaar te stellen voor bepaalde vormen van verwerking of voor latere communicatie. Alleen door een actieve ingreep van de gebruiker (bijvoorbeeld het invullen van een vinkje of het klikken op een knop voor toestemming) worden deze instellingen aangepast.

Zo zie je dat er allerlei manieren zijn om de privacy zo goed mogelijk te beschermen en de GDPR spoort iedereen aan deze altijd maximaal te gebruiken. Dataprivacy is dus geen eenmalig onderwerp voor een actueel project, dat we daarna weer kunnen vergeten. Het is een blijvende bekommernis.



11. GDPR – De onmiddellijke effecten

Sinds 25 mei 2018 is het zo ver. De General Data Protection Regulation (GDPR) of als je wil de 'Algemene Verordening Gegevensbescherming' (AVG) is van kracht geworden. De nieuwe Europese wet bepaalt nu hoe ondernemingen, overheden en organisaties moeten omgaan met persoonsgegevens. Laten we eens pragmatisch kijken wat er allemaal als een ware tsunami op ons af is gekomen in de afgelopen maanden.

Een van de eerste vaststellingen is hoe traag alles op gang kwam. Nochtans stond de GDPR niet plotseling voor de deur. Het was al jaren bekend dat deze wetgeving in de maak was en de officiële tekst is al gepubliceerd in april 2016. Verbazend dat er zo veel bedrijven niets of zeer weinig vanaf wisten en dat ze pas vanaf begin 2018 massaal zijn begonnen orde op zaken te stellen. Is dat een bewijs dat de meeste organisaties het niet zo nauw nemen met onze privacy en het beveiligen van de gegevens? Of was het toch echt onwetendheid?

Op twee terreinen merken we de meeste activiteit. Veel verantwoordelijken voor verwerking van persoonsgegevens hebben onder impuls van de GDPR contact gelegd met de individuele bestemmelingen in hun adressenbestanden of met andere personen over wie ze informatie verzamelen. Anderzijds wordt er druk onderhandeld tussen opdrachtgevers en bedrijven die voor hen persoonsgegevens behandelen. We bekijken beide fenomenen wat meer in detail.

11.1 Communicatie tussen verwerkingsverantwoordelijken en betrokkenen

In de aanloop naar **25 mei** en nadien is zowat iedereen overspoeld met mails of brieven van bedrijven en organisaties over data privacy. Soms vragen ze toestemming om je gegevens te gebruiken, soms melden ze gewoon dat hun privacy verklaring aangepast is, soms leggen ze uit wat ze over je weten en bewaren en waarom dat gerechtvaardigd is. Ongemerkt ging de datum in elk geval niet voorbij.

Het onbedoelde gevolg is dat onze mailbox vandaag vol zit met berichten waar we niet om gevraagd hebben en die ons vaak ook niet interesseren. Ze verstoren onze rust, maar verbeteren ze ook onze privacy?

Op zijn minst is het leerzaam vast te stellen wie allemaal gegevens over ons heeft. Daar zitten zeker en vast verrassingen tussen. Vaak is het niet duidelijk hoe onze contactgegevens bij een verantwoordelijke terechtgekomen zijn. Als we de moeite nemen om al deze communicatie te lezen, zijn we in ieder geval op de hoogte van de verwerkingen door deze firma's of organisaties. De transparantie is verhoogd – en dat was één van de doelstellingen van de GDPR.

Het is heel interessant om te zien hoeveel verschillende benaderingen er zijn. Veel campagnes hebben de bedoeling **toestemming te vragen aan de betrokkenen**.

- Soms gebeurt dit op een volstrekt nutteloze manier. Firma's schrijven betrokkenen aan omdat ze hun toestemming willen krijgen voor verwerking. Ze geven wat uitleg. En ze eindigen de communicatie met de stelling dat deze toestemming gegeven is tenzij de betrokkene contact opneemt om zich uit te schrijven. Dit is onder de GDPR zonder meer onwettig. Zwijgen is toestemmen kan niet meer. Er is een actieve handeling nodig en de verantwoordelijke moet ook kunnen aantonen dat hij een bewuste goedkeuring gekregen heeft. Zonder reactie is er dus geen rechtsgrond.

- Af en toe krijg je als betrokkene een echt mooie toepassing voorgeschoteld. Je kan doorklikken naar een site met veel informatie. Daar kan je alle elementen terugvinden die nodig zijn voor een correcte privacy verklaring: doel en rechtsgrond van de verwerkingen, bewaartermijn van de data en mogelijke bestemmelingen, beveiligingsmaatregelen… Soms krijg je ook de gegevens zelf te zien die de firma bewaart en heb je zelfs de mogelijkheid deze meteen te corrigeren of aan te vullen. En er is een duidelijke uitleg over je rechten en via welke weg je deze kunt uitoefenen. Uiteraard kan je ook verzoeken om de gegevens te verwijderen. Dit zijn de paradepaardjes van hoe het moet.
- Een grote vraag is wat er concreet gaat gebeuren met de verzoeken om toestemming waarop de betrokkene niet reageert. Wettelijk gezien moet het gevolg zijn dat de gegevens verwijderd worden en geen verdere communicatie meer gebeurt – de rechtsgrond waarvoor de verantwoordelijke gekozen heeft, is er immers niet. Gaan firma's hun poging om toestemming te vragen nog een paar keer herhalen? Tot wanneer is dat gerechtvaardigd? Dat zal de toekomst uitwijzen. En zullen we werkelijk geen verdere communicatie meer krijgen?
- Gaan we een turbo afslankcampagne ondergaan en megabytes aan berichten als sneeuw voor de zon zien verdwijnen? Helaas vrezen we dat het niet zo'n vaart zal lopen. De verstokte commerciële activiteiten zullen gewoon doorgaan, met of zonder GDPR. Je mag nu al concluderen dat de AVG of GDPR geen anti-spam filter is.

Andere verantwoordelijken kiezen bij het contacteren van de betrokkenen voor de tweede weg. Zij beroepen zich op **gerechtvaardigd belang**. In dat geval is geen toestemming van de betrokkene nodig, maar zorgt de communicatie ervoor dat de door de wet opgelegde transparantie er is. Als de campagne voldoende informatie geeft over de specifieke verwerking en de doelstelling ervan en als de betrokkene duidelijk te horen krijgt hoe hij zijn rechten kan uitoefenen en vooral hoe hij kan aangeven dat hij de verwerking niet wenst, is dit eveneens in orde voor de GDPR.

Een belangrijk aandachtspunt is wel het gebruik van persoonsgegevens voor **communicatie per email**. Daarop is niet enkel de GDPR van toepassing maar ook de zogenaamde **ePrivacy wetgeving,** een andere EU Richtlijn (2002/58/ec en 2009/136/ec). Het was de intentie van de EU om deze ook om te zetten in een nieuwe verordening en af te stemmen op de GDPR, maar mede door veel discussie en veel lobbywerk is deze herziening nog lang niet rond. Het is dan ook niet duidelijk welke richting het uiteindelijk zal uitgaan.

De huidige ePrivacy Richtlijn is strikter dan de GDPR en legt expliciet op dat toestemming van de betrokkene noodzakelijk is voor email-communicatie in een direct marketing context, tenzij de betrokkene een klantrelatie heeft en de aangeboden diensten of producten dicht aanleunen tegen reeds eerder verstrekte goederen of diensten. Nog recent is in Nederland door de beroepsorganisaties van marketeers gewezen op het gevaar dat hun business bedreigt als deze wetgeving te strikt zou worden.

Ook in deze situatie blijven natuurlijk wel de rechten van de betrokkene bestaan. Je kan altijd aan een firma het verzoek sturen om de verwerking van je gegevens stop te zetten, ook al vindt de verantwoordelijke dat hij een gerechtvaardigd belang heeft. Als er dan geen wettelijke verplichting speelt of een wettelijke bewaartermijn is opgelegd, moeten de gegevens verwijderd worden of op zijn minst de verwerking worden stopgezet. Dus ook als een organisatie kiest voor gerechtvaardigd belang als rechtsgrond, moet deze de nodige maatregelen uitwerken om dergelijke individuele verzoeken om stopzetting correct te kunnen doorvoeren. Dit is een hele klus.

11.2 Contracten en overeenkomsten tussen bedrijven

Een ander terrein waarop veel beweging merkbaar is, zijn de contractuele afspraken tussen verwerkingsverantwoordelijken en de firma's die zij als onderaannemer voor (delen van) de verwerking inschakelen. De GDPR schrijft immers voor dat de verantwoordelijke aansprakelijk blijft en er garant voor moet staan dat een leverancier die hij inschakelt zich eveneens terdege houdt aan zijn wettelijke verplichtingen. Dit moet aantoonbaar vastgelegd worden.

Uit eigen ervaring kunnen we melden dat het een titanenwerk is om met alle klanten en leveranciers waar nodig een Verwerkersovereenkomst af te sluiten. Hoewel er reeds vele organisaties hiermee zijn gestart, zijn er toch veel overeenkomsten nog altijd niet ondertekend.

Ook vanuit de Belgische federale regering via de diverse departementen is er reeds een poging ondernomen om alle verschillende soorten verwerkingsovereenkomsten te verzamelen en in een algemeen bruikbare template te steken voor alle steden en gemeentes binnen Vlaanderen. Maar tot op heden is er geen "one size fits all" oplossing gevonden. Het is ook bijzonder moeilijk om een echte standaard te hanteren. Van klanten kan je dit niet afdwingen, zeker niet als het grote organisaties zijn. Maar ook grote leveranciers schuiven hun eigen teksten naar voren. Onvermijdelijk volgt dan de fase om tientallen juridische stukken door te lezen en te screenen op volledigheid en evenwichtigheid.

Een aantal punten van discussie komen telkens terug.

- Kan aansprakelijkheid beperkt worden of niet? Alleen al de boetes kunnen gigantisch zijn, maar directe en vooral indirecte schade bij een ernstig datalek worden eveneens vaak zeer hoog ingeschat. Het lijkt redelijk dat de klant zijn leverancier niet wil doodnijpen, maar toch is het in veel gevallen niet zo simpel een beperking te bedingen tot bijvoorbeeld het verzekerde bedrag van een cybersecurity verzekering.
- Hoe ver moet het recht op audit reiken en wat met de kosten voor het ontvangen van een audit-delegatie?
- In hoeverre is het praktisch mogelijk het antwoorden op verzoeken van betrokkenen door te schuiven naar de onderaannemer. Is dat realiseerbaar bij een verwerker die bijvoorbeeld communicatiebatches uitstuurt?
- Is het redelijk dat een klant zijn leverancier oplegt om het even welke extra inspanning die uit de GDPR voortvloeit gratis te vervullen, omdat het nu eenmaal de wet is?
- Hoe moet je omgaan met het feit dat een verantwoordelijke aan een verwerker zijn specifieke goedkeuring moet geven om een subverwerker in te schakelen. Kan je je eigen bedrijfsvoering dan nog wel regelen.

Voor een aantal van deze punten zal gezocht moeten worden naar een evenwichtige regeling, op een economisch haalbare manier. Het is in ieder geval duidelijk dat slordigheid met persoonsgegevens streng zal kunnen afgestraft worden. Als verwerker kan je maar beter zorgen met de hoofdlijnen van de nieuwe wetgeving goed in orde te zijn. Net als kwaliteit zullen informatiebeveiliging en data privacy voortaan een onontkoombaar gegeven zijn voor elke firma die aan anderen diensten verleent waarbij verwerking van persoonsgegevens een rol speelt.

12. GDPR – Te verwachten gevolgen

In het vorige hoofdstuk bespraken we reeds de onmiddellijk merkbare effecten van het in werking treden van de GDPR. Een aantal andere belangrijke gevolgen die de invoering zou hebben, werden de voorbije twee jaar vooral aangehaald door juristen en consultants om business te creëren door te wijzen op grote bedreigingen: torenhoge boetes, een meldplicht van incidenten en datalekken, waarbij de melder misschien wel aan de schandpaal genageld zou worden, een toevloed van verzoeken van individuen die hun rechten op hun data zouden laten gelden... Tot nu toe kunnen we alleen maar constateren dat dit allemaal nog meevalt, maar dat is misschien omdat deze mechanismen slechts traag op gang komen. In elk geval zijn het op vandaag eerder de positieve gevolgen van de wet die zichtbaar worden.

12.1 Boetes

Hoe zit het eigenlijk met de boetes bij niet-naleving van de GDPR? Stel je eens de volgende vraag: "twintig miljoen euro of vier procent van de wereldwijde inkomsten van je bedrijf", wat betekent dit en welk van de twee is het grootst?

Laten we dit gegeven eens in perspectief plaatsen: 4% van Amazon's inkomsten (over 2016) zou 5,44 miljard dollar zijn en van Google 3,6 miljard dollar, van Facebook 1,1 miljard dollar en van Netflix, slechts 352 miljoen dollar. Je kunt zelf eens de berekening doen voor je eigen bedrijf.

Van de GDPR non-believers hoor je vaak de vergelijking met de beruchte millenniumbug tijdens de jaarovergang van 1999 naar het jaar 2000. Die werd ook wel de Y2K bug genoemd. Ook toen zou de wereld vergaan omdat vanaf 1 januari 2000 geen enkele computer zou blijven functioneren en we terug naar het stenen tijdperk zouden gekatapulteerd worden. Zo'n vaart is het gelukkig niet gelopen en de impact was relatief beperkt. Maar om deze situatie te gaan vergelijken met de AVG of GDPR is nogal kort door de bocht.

Toch zijn we inmiddels 25 mei 2018 gepasseerd en er is voor zover we weten tot op heden nog geen enkele boete uitgedeeld. Tot op heden is de Belgische Gegevensbeschermingsautoriteit (GBA), die de boetes moet bepalen en opleggen, overigens zelf ook nog niet klaar met de uitvoerende werkzaamheden om de nieuwe regelgeving toe te passen. Wil dit dan zeggen dat je op beide oren kunt slapen en er je als onderneming niets kan gebeuren? Dat zouden we zeker niet willen beweren.

12.2 Meldplicht van datalekken

Sinds 25 mei 2018 moeten binnen de EU alle datalekken van persoonsgegevens conform de GDPR gemeld worden. De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) aangifte moeten doen bij de Nederlandse Autoriteit Persoonsgegevens (AP) of de Belgische Gegevensbeschermingsautoriteit (GBA) zodra zij een ernstig datalek hebben – uiterlijk binnen de 72 uur nadat men in kennis gesteld is van het datalek. Als bedrijf heb je dus slechts drie dagen om incidenten bekend te maken aan de autoriteiten en een eventuele schending van de privacy te laten vaststellen.

Bij die aangifte zal je moeten uitleggen: 1) hoe het datalek is kunnen ontstaan; 2) welke maatregelen je zult nemen om te voorkomen dat het opnieuw kan gebeuren; 3) hoe en wanneer je gaat communiceren naar de betrokken partijen. Bij ernstige kans op schade moet je het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

In Nederland kent men deze meldplicht al sinds 2016 en het is daarom ook interessant om te zien hoeveel meldingen er zijn gedaan van mogelijke datalekken binnen organisaties.

Hieruit leren we dat er in 2017 ongeveer **10.000** meldingen zijn geregistreerd, waarvan **47 procent** werd veroorzaakt door persoonsgegevens te versturen of af te geven aan een verkeerde ontvanger.

De meest voorkomende gelekte gegevens waren: naam, adres, woonplaats, maar ook geslacht, geboortedatum en/of leeftijd en het rijksregister nummer. Opvallend is dat er **298** meldingen zijn ingetrokken omdat men achteraf vaststelde dat het geen echt datalek was. Voor de liefhebbers, het volledige rapport kan je als pdf downloaden op de website van de Nederlandse Autoriteit Persoonsgegevens.

Intussen is de meldplicht actief in alle deelstaten van de EU. Mocht je nieuwsgierig geworden zijn hoe dit juist in zijn werk gaat neem dan eens een kijkje op de site van de Belgische Gegevensbeschermingsautoriteit en probeer eens een melding van een (fictieve) datalek te registreren. Ik wens je alvast veel succes. In Nederland hebben ze dit bij de Autoriteit Persoonsgegevens (AP) al beter onder controle, maar die hebben dan ook ruim anderhalf jaar voorsprong met deze nieuwe meldplicht.

12.3 Uitoefening van de rechten van de betrokkenen

We weten ondertussen wat de rechten zijn van het data subject of met de officiële term in het Nederlands de betrokkene. Als ingezetene van de EU kan je bij elke organisatie een volledige lijst opvragen van alle gegevens die deze over je in haar bezit heeft. Bovendien kun je vragen deze informatie over te dragen in een transparante en voor iedereen leesbare vorm. Verder heb je het recht om vergeten te worden, behalve door de belastinginspecteur of als algemene wetgeving in je land hier anders over beslist. Denk maar aan boekhoudkundige informatie die minstens zeven jaar bewaard moet worden.De gegevensverzamelaar en/of gegevensverwerker heeft 30 dagen de tijd om te reageren op dergelijke verzoeken.

Maar wie van ons zal dit recht in de praktijk gaan toepassen, vraag ik me soms af. Tenzij je er plezier in schept bedrijven of verenigingen aan het werk te zetten door ze te laten uitzoeken (letterlijk) waar precies je informatie wordt bijgehouden. Misschien heb je wel valabele argumenten en er zullen vast wel omstandigheden zijn die hierom vragen. Maar het blijven wellicht de uitzonderingen die de regel bevestigen.

Ik geef toe dat het wat snel is om conclusies te trekken sinds de GDPR van kracht is, maar gaan we nu met zijn allen onze rechten laten gelden om onze informatie correct en veilig te laten bewaren bij derden in de Cloud? Maar wie gaat dit in onze naam straks allemaal telkens controleren? Vast niet de Belgische Gegevensbeschermingsautoriteit of de Nederlandse Autoriteit Persoonsgegevens (AP), want die hebben hun handen nu al vol.

Langs de andere kant zijn veel bedrijven op dit punt zeker nog niet goed voorbereid. Een recent onderzoek van Talend SA, waarvan Datanews en Techzine verslag uitbrachten, testte van juni tot begin september 2018 hoe bedrijven zouden reageren op verzoeken van betrokkenen om hun data te laten overdragen. Minder dan de helft voldeed aan de wettelijke voorschriften. Enkel een paar technologisch vooruitstrevende firma's hadden een mooie en snelle oplossing. Er is dus nog werk aan de winkel.

12.4 Positieve evoluties

We mogen trouwens daarnaast de positieve kanten van de GDPR niet vergeten. De nieuwe wetgeving is ook een kans om qua informatie binnen je bedrijf eens orde op zaken te stellen. Dit kan door eens kritisch naar de hoeveelheid aan data binnen je organisatie te kijken. En door een dataclassificatiesysteem toe te passen.

Vragen zoals: 'wie kan er aan deze informatie'? En 'waar bevindt deze informatie zich' zijn de eerste stappen in de goede richting om je informatiebeleid aan te passen. Ook de vraag 'waarom houden we deze specifieke persoonsgegevens bij en wat doen we ermee als bedrijf', kan bijdragen om het risico te verlagen bij een eventueel datalek. Immers voorkomen is altijd beter dan genezen. Op die manier ontstaat geleidelijk de reflex om eerst goed na te denken over de noodzaak om persoonsgegevens te verwerken, vooraleer te starten met het verzamelen.

Daarnaast merken we ook dat zowat alle bedrijven werk gemaakt hebben van hun privacy verklaring. Dankzij de GDPR en alle aandacht die er aan data privacy gegeven is, ontstaat een grotere openheid rond het verzamelen en verwerken van persoonsgegevens. Informatie daarover moet niet langer gezocht worden in de kleine lettertjes van contracten. Bedrijven maken er een punt van hun klanten en andere contactpersonen te melden welke gegevens ze over hen bijhouden en waarom dit nodig is.

Binnen veel organisaties is de gelegenheid ook aangegrepen om het personeel beter bewust te maken van risico's die kunnen leiden tot een inbreuk op de veiligheid van informatie. Niet enkel gesofisticeerde hacking 's bedreigen de gegevens waarvoor een bedrijf verantwoordelijk is, maar evengoed onoplettendheid of slordigheid van de eigen werknemers.

Hoe belangrijker data worden, hoe noodzakelijker het ook zal zijn het vertrouwen te krijgen van de eigenaars van de data bij het verwerken. Meer inzicht in het belang van data privacy en de mogelijke gevolgen van fouten dragen zeker bij tot een hoger niveau van veiligheid. Eens je orde op zaken hebt gesteld binnen je bedrijf qua informatiebeveiliging kan je dit kenbaar maken aan de hand van een soort van kwaliteitslabel. Zo kun je de professionele aanpak in het omgaan met persoons-herleidbare gegevens van je klanten – maar ook die van je eigen medewerkers – extra in de verf zetten.

13. GDPR – Obstakel in technologische ontwikkeling?

Naast alle andere effecten van de GDPR zouden er ook onbedoelde gevolgen kunnen zijn van het opleggen van deze nieuwe regelgeving op een van de meest winstgevende industrietakken van onze wereldeconomie, namelijk de technologische sector.

13.1 Bijkomende kosten, bijkomende voorwaarden voor start-ups

Ten eerste zullen de kosten stijgen, waardoor de winstgevendheid daalt met als gevolg minder winst en dus minder investeringen, minder startups en een langzamere groei van deze sector.

Nog een gevolg zou kunnen zijn dat de GDPR de toegang tot technologie voor inwoners en bedrijven in Europa zou kunnen gaan beperken. Veel applicaties worden tegenwoordig gemaakt door kleine bedrijven die op hun beurt heel wat persoonlijke informatie verzamelen. Elke internet-startup droomt ervan om hun eerste miljoen gebruikers aan zich te binden en trachten dit te bereiken door viraal te gaan met goedkope, vaak gratis software. Hun business model is het verzamelen van je gegevens om zo gebruik makende van Big Data waarde te creëren.

Maar nu vallen ze dus ook onder GDPR omdat ze persoonlijke gegevens over ingezetenen van de EU zullen bezitten en verwerken. De definitie van persoonlijke gegevens omvat onder andere ook je IP-adres, geo-locatie, huisadres en e-mailadres, die zeker worden verzameld. Hiervoor zal de internet-startup dus toestemming moeten vragen aan elke gebruiker.

13.2 Digitale grenzen

Sinds 2017 is er een gestage groei qua Cloud adoptie in België (zie ook onze Cloud Barometer) waarbij er inmiddels een op de vijf applicaties rechtstreeks vanuit de Cloud draaien. En 2018 zal het jaar worden dat bijna elke zichzelf respecterende KMO of MKB zich in Cloud oplossingen aan het verdiepen is, of zich laat begeleiden door hun IT huisleverancier met als opdracht om het maximale van de voordelen van Cloud oplossingen te kunnen benutten. Vaak krijgen we de vraag om daarin te kunnen adviseren daar de Cloud nog steeds niet voor iedereen even duidelijk is.

Een van de meest gestelde vragen is steevast: "is de Cloud wel veilig en hoe kan ik dit als bedrijfsleider controleren?" Vooral het verschil tussen Public en Private Cloud oplossingen is voor velen onduidelijk en zonder het zelf te beseffen zitten de meeste KMO's of MKB's al lang in de Public Cloud.

Menig werknemer heeft ondertussen wel een eigen privé e-mail of Dropbox account en heeft ook minstens één applicatie die als sociale media toepassing wordt gebruikt, denk daarbij aan Facebook of WhatsApp of LinkedIn. Dit bewijst vooral dat het gebruik van toepassingen uit de Cloud allang zijn ingeburgerd.

De meeste van deze toepassingen, zo niet alle, zijn afkomstig van Public Cloud providers uit de Verenigde Staten. Over dit fenomeen heb ik ooit ergens in de wandelgangen van een fabrikant het nu volgende gezegde opgevangen:

"Amerika vindt het uit (lees Amazon, Facebook, Google), China kopieert het (lees Alibaba, TenCent) en Europa regulariseert het (lees GDPR)".

Zeer toepasselijk als je ziet dat de grootste Public Cloud providers allemaal uit Amerika komen (Big 5) en al decennia lang hun diensten aanbieden, maar nu gaat Europa hier dus een stokje voor steken onder de noemer GDPR.

Maar als onderneming moet je kunnen aantonen dat je aan de in de vorige hoofdstukken besproken verplichtingen voldoet. Met name als het gaat om Clouddiensten, is iets als de GDPR een heet hangijzer, omdat de data van je bedrijf en hun gebruikers dan continu 'buiten het bereik' opgeslagen zullen worden.

Het nieuwe kader legt niet enkel verplichtingen op aan de verantwoordelijke voor de verwerking, maar ook aan partijen die verder in de keten de persoonsgegevens verwerken voor data-analytics, opslag, facturatie, … en dit laatste is toch een belangrijke nieuwigheid voor ICT-dienstverleners en meer specifiek de aanbieders van Clouddiensten. Deze privacy verordening voorziet dat men contracten moet aanpassen en data protection Policies moet opzetten, conform de vereisten van de verordening. Alle bedrijven zullen immers moeten kunnen aantonen dat zij op een verantwoorde manier omgaan met persoonsgegevens van medewerkers, klanten of toeleveranciers.

Hierdoor zijn er uitdagingen op verschillende niveaus. Veel bedrijven hebben – laten we eerlijk zijn – nooit stilgestaan bij gegevensbeveiliging. Technologie kan veel, maar applicaties en processen zullen herbekeken moeten worden in het licht van deze wetswijzigingen.

Een manier om dit te vermijden is gewoon geen gegevens over ingezetenen van de EU meer te verzamelen. Dat kan door de gebruikers op een knop te laten klikken waarbij ze bevestigen dat ze niet in de EU wonen voordat de app zal worden geïnstalleerd. Of door je geo-locatie te gebruiken om de app volledig te blokkeren.

Het gevolg hiervan zou kunnen zijn dat elke Europeaan zichzelf zal afsnijden van de nieuwste software ontwikkelingen. Wil je bijvoorbeeld de nieuwste beveiligde communicatie-app installeren? Sorry, dat zal niet (meer) gaan. Hoe zit het met die nieuwe zakelijke app voor het beheren van contacten of je administratie? Niet beschikbaar in de EU, alleen mensen buiten Europa kunnen er gebruik van maken.

Dit zou wel eens een groot probleem kunnen worden voor Europa. Begrijp me niet verkeerd want ik ben zelf groot voorstander van het verstandig omgaan met persoons herleidbare gegevens en de veiligheid van data opslag in het algemeen. Maar als de Belgische of Nederlandse gegevensbeschermingsautoriteit de regels van de GDPR letterlijk toepast, kunnen er nieuwe digitale grenzen ontstaan waar het internet en wij als consument niet op zitten te wachten.

14. ‘Voorlopig’ Besluit

De toekomst zal moeten uitwijzen hoe grote en kleine bedrijven, de individuele betrokkenen (misschien aangespoord door consumentenorganisaties of vakbonden), de toezichthoudende autoriteiten en de EU zelf met de GDPR zullen omgaan. Rechtbanken zullen zich ongetwijfeld over ingewikkelde geschillen moeten buigen. Het is dus moeilijk te voorspellen hoe de vele vragen die er momenteel nog zijn, zullen beantwoord worden. Daarom spreken we ook voorzichtig van een ‘voorlopig’ besluit. Maar één ding is duidelijk, dataprivacy is een begrip om rekening mee te houden en zal dat hoogstwaarschijnlijk ook blijven.

Eén doelstelling is in elk geval bereikt. Het afgelopen jaar heeft data privacy in elke vereniging, elke overheidsinstelling en elk bedrijf op de agenda gestaan. Iedereen heeft nagedacht over het gebruik van persoonsgegevens. In veel gevallen heeft dat geleid tot beslissingen om gegevensbestanden te reduceren of af te bouwen en om ze veel minder lang te blijven bewaren. Er wordt bewuster met deze gegevens omgegaan. Een sfeer van openheid rond deze thematiek is ontstaan. De gewenste transparantie is op veel plaatsen gecreëerd. Als de mediahype en de managementfocus eenmaal verdwenen zullen zijn, zal blijken of de resultaten blijvend zijn. Maar we hebben de indruk dat het alvast een verworvenheid is dat de betrokkenen het recht hebben te weten wat er met gegevens over hen wordt gedaan. Dit zit niet meer weggemoffeld in kleine lettertjes van ellenlange contracten maar staat klaar en duidelijk op websites, in mails en op apps geafficheerd.

Om stap voor stap alle onduidelijkheden weg te werken en te komen tot uniforme regels en afspraken, evenwichtige gedragscodes, meetbare controlemaatregelen, voor iedereen te gebruiken contractuele teksten is nog veel overleg nodig. Maar als we voortgaan op het werk dat in tal van organisaties momenteel al wordt verricht, kunnen we erop vertrouwen dat de huidige onzekerheid zal verminderen. De zorg voor data privacy zal, wellicht zoals kwaliteitsbeheer, milieuzorg en duurzaam ondernemen een vanzelfsprekendheid worden in de hele Europese Economische Ruimte.

Het moeilijkst te beantwoorden is de vraag of de hoofdbedoeling van de GDPR, namelijk evenwicht brengen tussen de bescherming van de persoonlijke levenssfeer en het recht op vrije meningsuiting en vrij verkeer van goederen en diensten, zal slagen. Als de regelgeving het opbloeien van nieuwe technologie op het domein van de kenniseconomie zou fnuiken of zelfs onmogelijk maken, slaat de wijzer te hard door in de ene richting. Als er van de verhoopte bescherming van de betrokkene in de praktijk niets in huis komt, is van evenwicht evenmin nog sprake.

Het wordt dus zoeken naar redelijkheid langs beide kanten, tussen betrokkenen en organisaties of bedrijven, tussen de Europese instellingen en de grote marktspelers, tussen inventieve startups, hun investeerders en hun klanten/gebruikers. En misschien niet in het minst tussen Europa en de andere wereldspelers – want we leven toch in een mondiale economie.

Reden genoeg dus om met veel belangstelling de ontwikkelingen te blijven volgen. Wij willen je graag op de hoogte houden van de verdere evolutie door middel van blogs en eventuele updates van het boek.

Over de auteur

Na een korte academische loopbaan stapte Viktor D'Huys[30] ruim 30 jaar geleden over naar de ICT-sector. Sinds 2003 is hij CIO van Group Joos en werkt hij mee aan de digitale transformatie van de groep, die evolueerde van een drukkerij en printshop naar een specialist in hybride communicatie, die ook tal van digitale diensten aanbiedt.

Hij specialiseerde zich onder meer in ICT-beveiliging. Hij zette het information security management system (ISMS) op waarmee Group Joos in 2013 het ISO 27001 certificaat kon behalen. Sinds 2016 kwam logischerwijze dataprivacy mee in het takenpakket. Samen met de data Protection Officer leidde hij het project dat Group Joos tijdig klaarstoomde voor de GDPR. Zijn blog over data privacy op de website van Group Joos ligt aan de basis van dit boek.

Hij is Certified Information Security Officer (CISM) en Certified Information Privacy Professional (CIPP/E).

Over de co-auteur

De voorbije tien jaar heeft Peter Witsenburg[31] de mogelijkheid gekregen om te werken in het domein van Cloud computing en van de informaticabeveiliging. In die laatste sector stond Peter in voor het uitvoeren van verschillende interne en externe audits op basis van ISMS en GDPR (regelgeving rond privacy en databescherming).

Onder andere bij Interxion heeft hij eveneens meegewerkt aan de implementering van de norm ISO27001 ISMS (Information Security Management System) met het oog op de risico-evaluaties, het informatiebeveiligingsbeleid en het business continuity plan (BCP) door gebruik te maken van de PDCA-methodiek.

Naast het werk is Peter vicevoorzitter van het selectiecomité van de vzw '*Netwerk Ondernemen Vlaanderen'.* In zijn vrije tijd schrijft hij graag artikels en blogs over de recentste ICT-trends. Bovendien is Peter de stichter van '*Belgium Cloud'* en de '*CloudMakelaar'.*

[30] De hoofdstukken 1 tot 10 zijn geschreven door Viktor D'Huys, met kleine retouches van Peter Witsenburg, die ook de schema's ter illustratie leverde.

[31] De hoofdstukken 11 tot 14 zijn een grondige herwerking van teksten van zowel Peter Witsenburg als Viktor D'Huys. De samenstelling en opmaak van het boek werden verzorgd door Peter Witsenburg.

Referenties

De **officiële wettekst** van de GDPR in het Engels, het Frans en het Nederlands kun je als PDF terugvinden via volgende links:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679

Achtergrond is overal te vinden. Ik beperk me hier tot enkele officiële kanalen.

De **Europese Commissie** geeft info via deze weg:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_nl

De website van de **Belgische Gegevensbeschermingsautoriteit** is op 25 mei 2018 aangepast. Met de oude URL (https://www.privacycommission.be) kom je nog op een overgangspagina, waar je de nieuwe site in het Nederlands, het Frans of het Engels kunt oproepen. De inhoud en opbouw van de site is ongeveer hetzelfde gebleven, maar geactualiseerd wat betreft de organisatie van de Gegevensbeschermingsautoriteit.

https://www.gegevensbeschermingsautoriteit.be/)

Deze site bevat veel informatie over de GDPR. Je vindt er een stappenplan, een hele reeks themadossiers en de mogelijkheid om documenten te downloaden.

https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-avg

De **Autoriteit Persoonsgegevens (AP)** is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

Hier kan u terecht op de site van de Autoriteit Persoonsgegevens (AP) en kan u een ruim aanbod vinden van nuttige informatie keurig gerangschikt per onderwerp.

GDPR - Verwijzingen artikels en overwegingen per hoofdstuk*

1.1.		Artikel 4.1 en 4.6 - Overweging 15, 26-27 en 30-31
1.2.		Artikel 4.13-15; Artikel 9-10 - Overweging 34-35 en 51-56
1.2	Pseudonimisatie	Artikel 4.5; Artikel 25 - Overweging 78
1.3	Gegevensverwerking	Artikel 2.1-2; Artikel 4.2
1.3	Huiselijke sfeer	Artikel 2.2c - Overweging 18
1.3	Verantwoordelijke	Artikel 4.7
1.3	Verwerker	Artikel 4.8
1.3	Betrokkene	Artikel 12
1.4		Artikel 37-39 - Overweging 97
2		Artikel 5 - Overweging 39
3.1		Artikel 30 - Overweging 82
3.1	Wie registerplicht	Artikel 30.5 - Overweging 13
3.2		Artikel 30.1 - Overweging 39
4.1		Artikel 6 - Overweging 40-50
4.1	speciale categorieën	Artikel 9 - Overweging 51-56
4.2		Artikel 4.11; Artikel 7-8 - Overweging 32-33,38,42-43
4.3		Artikel 6-9 - Overweging 47-49
5.1		Artikel 13-14 - Overweging 60-62
5.2		Artikel 12.1 - Overweging 58
6.1		Artikel 24.2 en 25; Artikel 32
6.2		Artikel 32; Artikel 35-36 - Overweging 75-76, 84, 89-95
6.3		Artikel 32 - Overweging 77-78
6.4		Artikel 28-29 - Overweging 79 en 81
7.1		Artikel 4.12; Artikel 33-34 - Overweging 75 en 87-88
7.2		Artikel 33 en 34 - Overweging 85-88
8.1		Artikel 12-15; Artikel 23 - Overweging 58-64
8.2		Artikel 16-23 - Overweging 65-73
9		Artikel 5.2; Artikel 24 - Overweging 74
10		Artikel 25 - Overweging 78

**Doorverwijzingen naar de GDPR Artikels met dank aan intersoft consulting, zie ook: gdpr-info.eu*

Alle artikels zijn in detail terug te vinden in het Engels in onderstaande publicatie:

Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016.

Nawoord: Group Joos en de GDPR

Persoonsgegevens verwerken is een van de kernactiviteiten van Group Joos. Daarom begonnen wij al in april 2016, nog voor de officiële publicatie van de GDPR met ons voorbereidingstraject. Er werd bijvoorbeeld meteen een Data Protection Officer (DPO) aangesteld. Wij vonden het immers onze plicht ten aanzien van onze klanten om meteen de nodige kennis op te bouwen en onze organisatie klaar te stomen om aan de nieuwe wetgeving te voldoen.

Het is voor Group Joos een absolute prioriteit om alle vertrouwelijke gegevens adequaat te beschermen. Daartoe behoren vanzelfsprekend alle persoonsgegevens. Wij hebben de afgelopen jaren zwaar geïnvesteerd in technologie en de nodige organisatorische maatregelen genomen om de informatiebeveiliging op het hoogste peil te brengen. Zo zijn wij al 5 jaar gecertificeerd voor ISO 27001.

Expertise en diensten van Group Joos

Wij zijn er dan ook van overtuigd dat Group Joos klaar is om als betrouwbare partner diensten te leveren aan zijn klanten waarbij persoonsgegevens verwerkt moeten worden.

Wie er zeker van wil zijn dat de persoonsgegevens waarvoor hij verantwoordelijk is, in goede handen zijn, is bij ons aan het juiste adres. Een reclamemailing uitvoeren, een multichannel campagne opzetten om prospecten te bereiken of zelfs documenten samenstellen met uiterst gevoelige medische of financiële informatie en deze afleveren aan de bestemmelingen via het kanaal van hun keuze. Wij zorgen ervoor dat de data veilig bij ons bezorgd kunnen worden, correct en vertrouwelijk verwerkt worden en hetzij op papier hetzij via één van de vele digitale kanalen veilig bij de bestemmeling afgeleverd worden. Desgewenst kunnen de data achteraf voor een afgesproken periode geëncrypteerd bewaard worden. Ook voor een betrouwbaar digitaal archief kan je bij ons terecht. Group Joos staat in voor een aangepaste technologische oplossing voor je communicatie en heeft een waaier aan mogelijkheden om je te helpen bij jouw digitale transformatie. Tegelijk zijn we klaar om dit te doen op een maatschappelijk verantwoorde manier en conform alle wettelijke bepalingen.

De expertise die we tijdens het voorbereidingstraject hebben opgebouwd, delen we graag met onze klanten en met alle geïnteresseerden. We hopen dat de informatie in deze publicatie iedereen van nut kan zijn die met vragen zit over het correct omgaan met persoonsgegevens.

GROUP JOOS Unlimited Digital Solutions & Print

Group Joos nv

Everdongenlaan 14 -2300 Turnhout (B)

gdpr@groupjoos.com www.groupjoos.com

HET GROTE

GDPR

HANDBOEK

Verantwoordelijke uitgever: Group Joos in samenwerking met de Cloud Makelaar