CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

WEGWIJS in de AVG voor KMO's

Een gids om kleine en middelgrote ondernemingen (KMO's) voor te bereiden op de Algemene Verordening Gegevensbescherming

januari 2018

Doel van dit document

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. De Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) wil KMO's informeren en bijstaan om deze nieuwe wetgeving te implementeren. Soms spreekt de brochure over de GBA, dit is de Gegevensbeschermingsautoriteit die de CBPL vanaf 25 mei 2018 zal vervangen.

Het is echter niet mogelijk om een brochure op te stellen die beantwoordt aan de specifieke noden van iedere individuele KMO. De impact van de AVG op het dagelijkse functioneren van een KMO hangt immers in de eerste plaats af van verwerkingsactiviteiten van die KMO en niet van het KMO-statuut op zich. De diversiteit aan verwerkingsactiviteiten die KMO's uitvoeren is te breed om te vatten in één enkel document.

Daarom nodigen we de sectorfederaties uit om dit basisdocument verder uit te werken en af te stemmen op de specificiteit van hun sector (in de vorm van templates, gedragscodes, richtsnoeren, etc.…). De CBPL is ervan overtuigd dat sectorfederaties het best geplaatst zijn om de concrete vertaalslag naar de sectorcontext te maken en de specifieke risico's per sector in kaart te brengen.

Deze brochure wil in vogelvlucht een overzicht geven van de voornaamste rechten en plichten die voortvloeien uit de AVG en die relevant zijn voor KMO's. De brochure heeft niet de ambitie om op exhaustieve wijze alle toepasselijke wetgeving te bespreken. De aangehaalde voorbeelden en de toelichting bij de AVG helpen om de AVG te begrijpen maar hebben geen juridische precedentwaarde. Bovendien vereist iedere toepassing van de AVG altijd een concrete analyse op maat van elke specifieke situatie.

Inhoudsopgave

Begrippenlijst

AVG	De Algemene Verordening Gegevensbescherming
CBPL	De Commissie voor de Bescherming van de Persoonlijke Levenssfeer
GBA	De Gegevensbeschermingsautoriteit. Op 25 mei 2018 volgt de GBA de Commissie voor de Bescherming van de Persoonlijke Levenssfeer op als toezichthoudende autoriteit.
WP29	De Groep Gegevensbescherming artikel 29. De groep omvat de nationale toezichthouders, waaronder de CBPL, en geeft advies over de toepassing van de Europese privacywetgeving. Vanaf 25 mei 2018 vervangt het Europees Comité voor gegevensbescherming de Groep Gegevensbescherming artikel 29.
DPO	De functionaris voor gegevensbescherming – in het Engels ook wel Data Protection Officer (DPO) genoemd.
GEB	De gegevensbeschermingseffectbeoordeling – in het Engels ook wel Data Protection Impact Assessment (DPIA) genoemd.
Inbreuk in verband met persoonsgegevens	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens – in het Engels ook wel Data Breach genoemd.

Inleiding

De AVG voert één geharmoniseerde privacywet in die direct van toepassing is binnen heel de Europese Unie. In beginsel is de AVG op dezelfde wijze van toepassing in de publieke en private sector en geldt deze wetgeving voor zowel grote bedrijven als KMO's. Let op: Op verschillende vlakken kunnen EU-lidstaten specifieke nationale wetgeving aannemen om de AVG verder uit te werken of uitzonderingen te maken. Houd naast de AVG dus ook steeds rekening met specifieke nationale wetgeving. Het gaat hierbij niet uitsluitend om gegevensbeschermingsrecht maar ook om andere rechtsdomeinen, zoals bijv. het arbeidsrecht, die worden beïnvloed door de AVG.

De nieuwe AVG bouwt verder op de huidige wetgeving. De basisconcepten en principes die aan de basis liggen van de verwerking van persoonsgegevens, blijven grotendeels behouden. Indien uw KMO voldoet aan de Belgische wet tot bescherming van de persoonlijke levenssfeer, bent u al goed op weg om ook de AVG na te leven. De AVG voegt hier een aantal nieuwe elementen aan toe om de wetgeving in lijn te brengen met de snelle technologische ontwikkelingen van de afgelopen twintig jaar.

De nieuwe verplichtingen die de AVG met zich meebrengt laten zich samenvatten in drie krachtlijnen: de risico-gebaseerde aanpak, verantwoordingsplicht en transparantie:

- ***De risico-gebaseerde aanpak*** betekent dat sommige verplichtingen die voortvloeien uit de AVG variëren in functie van het risico dat verbonden is aan de verwerkingsactiviteit. De AVG creëert dus ruimte om tot een oplossing op maat te komen voor iedere KMO.

- ***De verantwoordingsplicht*** houdt in dat een verwerkingsverantwoordelijke de naleving van de AVG moet kunnen aantonen. Daarom is het documenteren van keuzes belangrijk zodat een KMO kan verantwoorden waarom het een bepaalde maatregel al dan niet invoerde.

- ***Transparantie*** is van cruciaal belang, zowel intern als extern. Intern moet u een duidelijk beeld hebben van alle verwerkingen van persoonsgegevens binnen uw KMO en moet u het personeel hierover sensibiliseren. Extern, moet u de personen wiens gegevens u verwerkt helder informeren over hun rechten, de manier waarop zij die rechten kunnen uitoefenen en het hoe en waarom van de verwerkingsactiviteit.

Deze brochure is in de eerste plaats geschreven vanuit het perspectief van de KMO als verwerkings-verantwoordelijke. De verplichtingen die gelden voor verwerkingsverantwoordelijken en verwerkers zijn niet identiek. Daarom verduidelijkt titel V Checklist voor de verwerker kort welke verplichtingen gelden voor verwerkers. Let op: uw KMO kan soms zowel verwerkingsverantwoordelijke als verwerker zijn. Voor meer informatie over de begrippen verwerker en verwerkingsverantwoordelijke, zie titel I Basisbegrippen.

I. Basisbegrippen – verwerk ook ik persoonsgegevens?

De AVG is van toepassing indien uw KMO *persoonsgegevens verwerkt*.

- **Persoonsgegevens** zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4.1 AVG). Gegevens die toelaten om een natuurlijke persoon rechtstreeks of onrechtstreeks te identificeren vallen hier ook onder. Wanneer het koppelen van puzzelstukjes van informatie (leeftijd, geslacht, postcode, etc.) kan leiden tot de unieke identificatie van een persoon ('singling out'), is elk puzzelstukje ook een persoonsgegeven. Gepseudonimiseerde[1] persoonsgegevens waarvoor een sleutel bestaat om de oorspronkelijke persoonsgegevens opnieuw te verkrijgen, zijn ook persoonsgegevens. Anonieme gegevens[2] en gegevens over overleden personen of rechtspersonen zijn geen persoonsgegevens.

o **VOORBEELD:**

Zijn wel persoonsgegevens:

- naam, voornaam en contactgegevens van klanten, personeel of leveranciers;
- historiek van aankopen, openstaande facturen, betalingsinformatie (voor zover zij betrekking hebben op natuurlijke personen);
- personeelsevaluaties en ziektebriefjes;
- informatie over de webpagina's die een IP-adres bezoekt;
- locatiegegevens (bv. lokalisatie via een Smart Phone app);
- lijst van de personeelsnummers die halftijds werken;
- camerabeelden en nummerplaten.

Zijn geen persoonsgegevens:

- algemeen E-mailadres of telefoonnummer van de KMO – bijv. KMO@email.be;
- ondernemingsnummer (behalve bij een éénmanszaak).

- **Gevoelige gegevens** zijn persoonsgegevens die een hoger beschermingsniveau verdienen omdat hun verwerking significante risico's met zich mee kan brengen. De verwerking van gevoelige gegevens is in beginsel verboden, tenzij u aan één van de uitzonderingsgronden van artikel 9 of 10 van de AVG voldoet. Ook gewone persoonsgegevens waaruit u gevoelige informatie kan afleiden zijn gevoelige gegevens. Het gaat om:

  - bijzondere categorieën van persoonsgegevens (artikel 9 AVG). Tot deze groep behoren gezondheidsgegevens, genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een persoon. Persoonsgegevens waaruit ras of etnische afkomst, seksuele gerichtheid en gedrag, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken behoren ook tot deze bijzondere categorie;
  - gerechtelijke gegevens over strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG) .

o **VOORBEELD:**

  - een sportapp die snelheid, afstand, hartslag en calorieverbranding meet, kan informatie onthullen over de gezondheidstoestand van een persoon;
  - een uittreksel van het strafregister.

- **Het begrip verwerking** is zeer ruim en omvat iedere bewerking van persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés (artikel 4.2 AVG). Voorbeelden van verwerking zijn het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

  ⚠ Hoewel de AVG in de eerste plaats geautomatiseerde verwerkingen van persoonsgegevens beoogt (zoals bijv. de opslag op een digitale drager), kan u de wet niet omzeilen door alle persoonsgegevens op papieren dragers te bewaren. Het bijhouden van systematisch geordende bestanden op papier is ook een verwerking in de zin van de AVG.

1 De AVG gebruikt de term pseudonimisering om te verwijzen naar gecodeerde gegevens die niet meer aan een specifieke natuurlijke persoon kunnen worden gekoppeld zonder aanvullende gegevens als sleutel.

2 In tegenstelling tot gepseudonimiseerde persoonsgegevens bestaat voor anonieme gegevens geen sleutel meer om de natuurlijke persoon te identificeren. Een voorbeeld hiervan zijn geaggregeerde, statistische gegevens.

- **VOORBEELD:**

  - het verzamelen van klantengegevens via een webpagina om online aankoop te verrichten;
  - het bijhouden van systematisch geordende papieren fiches met klantengegevens;
  - het digitaal opslaan, raadplegen en beheren van HR-gegevens van uw personeel.

- Het is ook belangrijk de **actoren** te bepalen waarop de AVG van toepassing is. De instantie die het doel en de middelen voor de verwerking bepaalt, is de **"verwerkingsverantwoordelijke"**(artikel 4.7 AVG). De onderneming die in dienst van een verwerkingsverantwoordelijke persoonsgegevens verwerkt noemen we de **"verwerker"** (artikel 4.8 AVG). Identificeerbare of geïdentificeerde personen van wie persoonsgegevens worden verwerkt, zoals klanten of personeel, worden in dit document ook aangeduid door de term **"betrokkene"** (artikel 4.1 AVG). Overleden personen of rechtspersonen worden niet als "betrokkenen" beschouwd.

- **VOORBEELD:**

  - een KMO is de verwerkingsverantwoordelijke van zijn klanten- en personeelsgegevens;
  - een sociaal secretariaat dat HR-gegevens verwerkt voor andere bedrijven is vaak verwerker;
  - een cloud provider waarop een KMO beroep doet om gegevens op te slaan, is vaak een verwerker.

Voor meer info

- Artikel 4 AVG – Definities
- *Advies 4/2007* van de WP 29 over het begrip persoonsgegeven – WP 136

II. Plichten – waar moet ik rekening mee houden?

De AVG is van toepassing op iedere verwerking van persoonsgegevens en maakt hier in principe geen uitzonderingen op voor KMO's. Een KMO moet dus steeds de basisprincipes respecteren die aan de grondslag liggen van elke rechtmatige verwerking van persoonsgegevens (Titel II.1 Basisprincipes).

Dit betekent niet dat de AVG de lat voor elke KMO even hoog legt. Sommige maatregelen hoeft een KMO slechts te nemen indien een verwerking gepaard gaat met bijzondere risico's, zoals bijvoorbeeld het aanstellen van een functionaris voor de gegevensbescherming (DPO) of het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB). (Titel II.2 Beschermingsmaatregelen afgestemd op de risico's)

Daarnaast wijst dit hoofdstuk op de plichten van de verwerker en de verwerkingsverantwoordelijke, indien deze laatste beroep doet op een externe dienstverlener - een verwerker dus - (outsourcing). Het verwerken van gegevens in de Cloud of een datacenter, maar ook het uitbesteden van personeelsadministratie zijn hiervan courante voorbeelden. (Titel II.3 Externe dienstverleners).

Tot slot moeten KMO's bijkomende waarborgen in acht nemen bij de doorgifte van persoonsgegevens buiten de Europese Unie (Titel II.4 Waar gaan uw gegevens naartoe?).

1 Basisprincipes

1.1 Rechtsgrond

Elke verwerking van persoonsgegevens moet steunen op één van de rechtsgronden die artikel 6 van de AVG opsomt. De AVG onderscheidt zes verschillende rechtsgronden: toestemming, overeenkomst, naleven van een wettelijke verplichting, behartiging van een vitaal belang, uitvoering van een taak van openbaar belang en het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

Een KMO zal zich voornamelijk beroepen op **de toestemming, de overeenkomst, de naleving van een wettelijk verplichting** en **het gerechtvaardigd belang**. Al deze rechtsgronden zijn gelijkwaardig en het komt aan de KMO toe om de rechtsgrond te kiezen die het best aansluit bij haar verwerkingsactiviteiten.

⚠ Let op: als u gevoelige gegevens verwerkt moet u bovenop één van deze rechtsgronden ook voldoen aan één van de uitzonderingsgronden in artikel 9.2 of artikel 10 AVG!

TO DO

Documenteer v oor elke verwerking de rechtsgrond.

Voor meer info

- ❖ Artikel 6 AVG – Rechtmatigheid van de verwerking
- ❖ Artikel 9 AVG – Verwerking van bijzondere categorieën van persoonsgegevens
- ❖ Artikel 10 AVG – "Verwerking van persoonsgegevens m.b.t. strafrechtelijke veroordelingen

1.1.1 De toestemming

Een KMO mag persoonsgegevens verwerken indien de betrokkene hierin toestemt. Wees echter gewaarschuwd: de toestemming is geen mirakeloplossing die samenvalt met een aanvaarding van de algemene voorwaarden! Bovendien mag de betrokkene zijn of haar toestemming altijd en zonder enige motivering intrekken.

Volgens de definitie in artikel 4.11 van de AVG moet iedere toestemming:

- **vrij** zijn. De betrokkenen moeten een *echte* keuze hebben zonder dat zij onder druk worden gezet met negatieve gevolgen indien zij hun toestemming niet zouden geven. Een toestemming die onlosmakelijk verbonden is aan de aanvaarding van algemene voorwaarden, is niet geldig.
    - o **VOORBEELD**:
    - – in de relatie tussen een werkgever en werknemer zal toestemming zelden vrij zijn door de gezagsverhouding die tussen hen beiden bestaat;
    - – een KMO ontwikkelt een app die gebruikers ondersteunt om talen te leren. Gebruikers moeten bij de installatie de app de toelating geven om hun GPS-lokalisatie te activeren als voorwaarde om de app te gebruiken. De KMO wendt deze informatie aan voor commerciële doeleinden. Geolokalisatie van de gebruiker is echter niet noodzakelijk voor het functioneren van de app. Aangezien de gebruiker de app niet kan gebruiken zonder in te stemmen met de geolokalisatie, is de toestemming niet vrij.

- **specifiek** zijn. Dit betekent dat de betrokkene voor ieder afzonderlijk doeleinde de keuze moet hebben om al dan niet in te stemmen.
    - o **VOORBEELD**: een KMO vraagt één toestemming om klanten op de hoogte te houden van nieuwe aanbiedingen én om hun klantengegevens te delen met commerciële partners. Deze toestemming is niet specifiek omdat je niet afzonderlijk kan instemmen met (één van) beide doelstellingen.
- **geïnformeerd** zijn. Dit betekent dat de KMO vooraf in begrijpelijke taal de betrokkene moet uitleggen wie, welke persoonsgegevens voor welke doeleinden zal gebruiken. Een KMO moet de betrokkene ook altijd wijzen op de mogelijkheid om de toestemming in te trekken. Al deze informatie moet duidelijk te onderscheiden zijn van alle andere informatie of contracts-bepalingen.
    - o **VOORBEELD**: een paragraaf in de algemene voorwaarden met informatie over de verwerking van persoonsgegevens leidt niet tot een geïnformeerde toestemming.
- berusten op een **positieve actie**.
    - o **VOORBEELD:** de toestemming mag niet worden afgeleid uit een vooraf aangevinkt vakje op een formulier (opt-out).

Daarnaast moet een geldige toestemming ook voldoen aan een aantal bijkomende vereisten. Zo moet de toestemming ook:

- **aantoonbaar** zijn. U moet steeds een bewijs bewaren van het verkrijgen van de toestemming.
- **even gemakkelijk kunnen worden ingetrokken als ze werd gegeven.**
    - o **VOORBEELD:** bij een online aankoop stemt een klant in om reclame te ontvangen van de KMO door een vakje aan te kruisen. Om die toestemming in te trekken moet de klant de KMO opbellen. Aangezien de drempel om te bellen hoger is dan een muisklik, is de toestemming ongeldig.

Toestemming die onder Belgische privacywetgeving werd gegeven blijft slechts geldig in zoverre die in overeenstemming is met de AVG!

- **VOORBEELD**: u verzamelde de toestemming om persoonsgegevens te verwerken via een vooraf aangevinkt vakje. Onder de AVG is dit niet meer mogelijk! U moet dus een nieuwe toestemming vragen aan de betrokkene vóór 25 mei om verder te gaan met de verwerking.

⚠ Let op: u kan gevoelige gegevens ook verwerken op basis van de toestemming. In dit geval moet de toestemming ook 'uitdrukkelijk' zijn. De lat voor een uitdrukkelijke toestemming ligt hoger dan voor een gewone toestemming en vereist een uitdrukkelijk verklaring van toestemming. Dit kan bijv. door middel van:

- een (elektronisch) ondertekende digitale of schriftelijke verklaring van de betrokkene;
- door een dubbele bevestiging via mail en/of SMS (double opt-in)

Voor meer info

- Artikel 7 AVG – Voorwaarden voor toestemming
- Artikel 4.11 AVG – Definities
- Richtlijnen van de WP29 over toestemming onder Verordening 2016/679 – WP259

1.1.2 De overeenkomst

Een KMO mag bij het afsluiten van een contract de persoonsgegevens van een klant, personeelslid of leverancier verwerken die noodzakelijk zijn voor de uitvoering van dat contract. Deze rechtsgrond dekt ook precontractuele maatregelen voor zover die op verzoek van de betrokkene worden uitgevoerd. Het initiatief moet dus bij de betrokkene liggen. Deze noodzakelijkheid is niet ruim te interpreteren en beperkt zich tot die persoonsgegevens zonder dewelke de overeenkomst niet uitgevoerd *kan* worden.

- **VOORBEELD:**

  - een KMO moet als werkgever persoonsgegevens van haar werknemers verwerken om het loon uit te betalen. Deze verwerking is noodzakelijk om de arbeidsovereenkomst uit te voeren;
  - een klant vraagt een KMO om een offerte. Om deze offerte op te sturen en in afwachting van de aanvaarding ervan mag de KMO op basis van deze rechtsgrond de contactgegevens van de toekomstige klant tijdelijk bewaren;
  - bij de online verkoop van goederen mag een KMO persoonsgegevens verwerken zoals bv. de naam, adresgegevens en kredietkaartgegevens om de betaling en levering mogelijk te maken;
  - bij de online verkoop van goederen volstaat deze rechtsgrond niet om een gebruikersprofiel op te stellen op basis van het aankoop- en klikgedrag van de gebruiker. Hoewel deze informatie de KMO misschien een economisch voordeel kan opleveren, zijn deze persoonsgegevens niet noodzakelijk voor de uitvoering van de aankoopovereenkomst zelf.

⚠ Let op: als u gevoelige gegevens verwerkt, kan uw verwerking niet steunen op deze rechtsgrond!

1.1.3 De wettelijke verplichting

Een KMO mag persoonsgegevens verwerken als de wet dit oplegt. Voor een KMO is deze rechtsgrond bv. van belang om persoonsgegevens van personeelsleden aan te geven bij de fiscus of de instellingen van de sociale zekerheid

- **VOORBEELD:** het koninklijk besluit van 5 november 2002 tot invoering van een onmiddellijke aangifte van tewerkstelling (DIMONA-aangifte) schrijft voor dat de werkgever persoonsgegevens van een werknemer aan de Rijksdienst voor Sociale Zekerheid communiceert. De overheid gebruikt deze gegevens om bepaalde sociale rechten toe te kennen aan de werknemer.

⚠ Let op: als u gevoelige gegevens verwerkt, moet de wettelijke verplichting in kwestie vallen onder één van de categorieën van artikel 9.2 AVG!

1.1.4 Het gerechtvaardigde belang van de verwerkingsverantwoordelijke

Een KMO mag persoonsgegevens verwerken als dit noodzakelijk is voor een gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene zwaarder doorwegen. Dit betekent dat de KMO in de eerste plaats een gerechtvaardigd belang moet nastreven om vervolgens een afweging te maken met de belangen van de betrokkene. Deze rechtsgrond is dus dynamisch en vraagt voor iedere verwerking een bijzondere en gedocumenteerde rechtvaardiging die de noden van de KMO afweegt aan de impact op de betrokkene.

- **VOORBEELD:**

  – direct marketing is een courante methode om aan klantenprospectie te doen. Als de direct marketing niet te frequent en agressief is, mag de KMO binnen een bestaande klantenrelatie contactgegevens gebruiken voor direct marketing om haar eigen diensten of producten aan te prijzen. Let op: artikel 13 van de e-Privacyrichtlijn (Richtlijn 2002/58/CE)[3] legt een aantal extra voorwaarden op. Bij de inzameling van de contactgegevens moet de KMO de klant expliciet wijzen op het recht om zich tegen direct marketing te verzetten. De KMO moet het gemakkelijk maken om dat recht uit te oefenen (bijv. via een duidelijke zichtbare 'opt-out' mogelijkheid bij de inzameling van de gegevens en bij iedere direct marketing communicatie).
  – op basis van deze rechtsgrond mogen KMO's persoonsgegevens verwerken die noodzakelijk zijn om factuurfraude te detecteren en hun klanten hiervan op de hoogte te brengen.

⚠ Let op: als u gevoelige gegevens verwerkt, kan uw verwerking niet steunen op deze rechtsgrond!

1.2 Doeleinde

Het principe van doelbinding is een cruciaal fundament van de AVG. Volgens artikel 5.b AVG mag u persoonsgegevens uitsluitend verwerken voor doeleinden die vooraf uitdrukkelijk zijn vastgelegd. In beginsel – maar hierop bestaan uitzonderingen – is het verboden om de verkregen gegevens nadien verder te verwerken voor een ander doel dat oorspronkelijk niet was voorzien. Dit is het basisprincipe.

Drie mogelijkheden dienen zich aan als u toch persoonsgegevens wil verwerken voor een doeleinde dat afwijkt van het doeleinde waarvoor u deze gegevens oorspronkelijk verkreeg:

- **Afzonderlijke toestemming**: u vraagt de toestemming van de betrokkene om de persoonsgegevens te verwerken voor dit nieuwe doeleinde. Deze toestemming vormt dan de rechtsgrond van de verwerking voor dit nieuwe doeleinde;

  - **VOORBEELD**: een KMO ontwikkelt een klantenprofiel op basis van het aankoop- en klikgedrag op haar website. De klant stemde hiermee in om zijn gebruikservaring te optimaliseren en op de hoogte te blijven van bijzondere aanbiedingen waarin hij of zij geïnteresseerd zou kunnen zijn. Als de KMO deze profielen later wil doorverkopen aan een data broker voor advertentiedoeleinden, moet zij hiervoor apart de toestemming van de klant vragen.

- **Wettelijke verplichting**: de verdere verwerking van persoonsgegevens vloeit voort uit een wettelijke verplichting. De wettelijke verplichting maakt in dit geval de rechtsgrond uit van de verdere verwerking;

- **Verenigbaarheid**: de verwerkingsverantwoordelijke moet beoordelen of het nieuwe doeleinde ***verenigbaar*** is met de doeleinden waarvoor de gegevens oorspronkelijk werden verkregen. Zo ja, dan is de verwerking gesteund door de rechtsgrond op basis waarvan u de gegevens oorspronkelijk verkreeg en verwerkte.

  - **VOORBEELD**:

  – een KMO installeert een bewakingscamera aan de ingang van haar winkel. De camera filmt toevallig ook de kassierster die de klanten onthaalt en telefoons aanneemt. De KMO mag die camerabeelden in principe enkel gebruiken bij een veiligheidsincident (bv. een overval) en niet om de arbeidsprestaties van de kassierster te evalueren.

De AVG somt enkele criteria op die kunnen helpen om na te gaan of het nieuwe doeleinde al dan niet verenigbaar is met het oorspronkelijke doeleinde. Deze criteria gaan na of deze verdere verwerking redelijkerwijze voorzienbaar was voor de betrokkene. De KMO moet aldus rekening houden met:

3 Op het moment van schrijven is de e-Privacyrichtlijn onder herziening. De Europese Commissie heeft initiatief genomen om de e-Privacyrichtlijn om te vormen tot een e-Privacyverordening. Deze regel kan in de toekomst dus mogelijk wijzigen.

- het verband tussen de oorspronkelijke doeleinden en de nieuwe doeleinden;
- de context waarin de persoonsgegevens werden verkregen en in het bijzonder de relatie tussen de betrokkenen en de verantwoordelijke voor de verwerking;
- de gevoeligheid en de aard van de persoonsgegevens, vooral als de verwerking slaat op bijzondere categorieën persoonsgegevens;
- de mogelijk gevolgen van de verdere verwerking voor de betrokkenen;
- het bestaan van passende waarborgen, waaronder versleuteling of codering.

o **VOORBEELD:** een KMO levert verse bereide maaltijden met lokale ingrediënten aan huis. De KMO wil de contactgegevens en aankoopgeschiedenis gebruiken om bijzondere aanbiedingen of een korting op haar eigen maaltijden toe te passen. Dit gebruik is verenigbaar met het oorspronkelijke doeleinde aangezien er een nauwe band bestaat tussen de dienstverlening en de bijzondere aanbiedingen, de gegevens niet gevoelig zijn en de gevolgen voor de klant positief zijn. Let op, deze analyse kan anders uitdraaien indien de KMO gebruik maakt van verregaande profilering of wanneer dit leidt tot prijsdifferentiatie.[4]

TO DO

Controleer of elke verwerking van persoonsgegevens een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde heeft en dat, indien die gegevens hergebruikt worden voor een ander doeleinde dan het oorspronkelijke doeleinde, het nieuwe gebruik van de gegevens verenigbaar is met het eerste gebruik.

Voor meer info

- ❖ Artikel 5.1.b) AVG – Beginselen inzake verwerking van persoonsgegevens
- ❖ Artikel 6.4 AVG – Rechtmatigheid van de verwerking
- ❖ Advies 03/2013 van de WP 29 over doelbinding – WP 203

1.3 Juistheid en gegevenskwaliteit

De persoonsgegevens moeten juist en actueel zijn. Zodra een KMO zich bewust wordt van het foutieve of gedateerde karakter van de persoonsgegevens, moet ze deze actualiseren, verbeteren of wissen. Hoewel een KMO niet de eindverantwoordelijkheid draagt indien een klant of een andere betrokkene foute informatie verstrekt, moet ze wel proactieve inspanningen leveren om voor de hand liggende fouten te detecteren en recht te zetten. De betrokkene heeft trouwens ook een recht op de verbetering van zijn persoonsgegevens (zie hiervoor Titel III. Rechten van de betrokkene).

Dit beginsel heeft ook gevolgen voor de bewaartermijn van persoonsgegevens. Indien u gegevens te lang bewaart, zijn deze niet langer accuraat. Stippel dus een beleid uit waarbij oude persoonsgegevens systematisch gewist of geactualiseerd worden.

o **VOORBEELD:**

– wanneer een klant of personeelslid een wijziging meedeelt, moet de KMO deze wijziging zo snel mogelijk doorvoeren. Die wijziging kan gaan over naam, adres, woonplaats, emailadres, telefoonnummer, aantal kinderen ten laste, nummerplaat etc.....

TO DO

Controleer actief uw klantengegevens om foute e-mailadressen te detecteren en de match tussen postcode en straatnaam te verifiëren. Contacteer uw klant indien u vermoedt dat de gegevens foutief zijn en pas zo nodig aan.

Voor meer info

- ❖ Artikel 5.1.d) AVG – Beginselen inzake verwerking van persoonsgegevens
- ❖ Artikel 16 AVG – Recht op rectificatie

4 Zoals hoger vermeld moet de KMO de klant uitdrukkelijk informeren dat deze het recht heeft om zich tegen de direct marketing te verzetten en het voor de klant gemakkelijk maken om dat recht uit te oefenen.

1.4 Minimale gegevensverwerking

De verzameling en verwerking van persoonsgegevens moeten zich beperken tot wat strikt noodzakelijk is om de vooropgestelde doeleinden te vervullen. De opgevraagde gegevens moeten pertinent zijn. Dit betekent dat een KMO voor ieder persoonsgegeven moet kunnen aantonen waarom die informatie noodzakelijk is om het doeleinde te bereiken. Kan de KMO dit niet aantonen, dan zijn de persoonsgegevens overbodig en moeten ze gewist worden.

- **VOORBEELD:**
  - een KMO gebruikt een ERP-software (Enterprise Resource Planning) om haar klantenbestand te beheren. De ERP-software voorziet in vrije velden om extra informatie over de relatie met de klant te registreren en de dossieropvolging te vergemakkelijken. Registreer geen excessieve informatie in dit vrije veld! Bij een betalingsachterstand is de opgave van de bepaalde redenen hiervoor zoals "*klant is gescheiden*" of "*klant is werkloos*" niet pertinent;
  - een KMO die iemand aanwerft moet een aantal gegevens kennen met betrekking tot de sociale zekerheid, gezinssituatie, behaalde diploma's. De werkgever mag uitsluitend de gegevens bewaren die noodzakelijk zijn voor de professionele band met de medewerker. De KMO mag dus geen medische gegevens bewaren, zoals bijvoorbeeld dat hij of zij in een welbepaald jaar een longontsteking had en het slachtoffer was van een beenbreuk. De KMO mag wel het aantal dagen optekenen tijdens welke de medewerker afwezig was wegens ziekte.

TO DO

Sorteer de verwerkte gegevens en stel steeds de vraag of er nog een werkelijke nood bestaat om de gegevens te verwerken. Misschien kan u hetzelfde doel met minder gegevens of minder gevoelige gegevens bereiken.

Voor meer info

- Artikel 5.1.c) AVG – Beginselen inzake verwerking van persoonsgegevens

1.5 Bewaartermijn

Een KMO mag persoonsgegevens nooit langer bewaren dan noodzakelijk is om de vooropgestelde doeleinden te bereiken. Zodra deze doeleinden zijn volbracht of wegvallen, moet een KMO de persoonsgegevens wissen. Immers, bij gebrek aan een doeleinde valt de noodzaak tot het bewaren en verwerken weg. Daarom moet een KMO maximale bewaartermijnen vastleggen voor al haar persoonsgegevens. Soms heeft de wetgever zelf al een verplichte bewaartermijn vastgelegd.

- **VOORBEELD**:
  - persoonsgegevens die zijn opgenomen in de boekhouding, moet een KMO pas na zeven jaar wissen. Artikel III.88 van het Wetboek Economisch Recht bepaalt dat ondernemingen hun boeken moeten bewaren gedurende 7 jaar. Dezelfde redenering gaat op voor documenten, zoals facturen, die de KMO moet bewaren door BTW wetgeving of voor directe belastingen;
  - een KMO moet de persoonsgegevens van een sollicitant verwijderen van zodra het duidelijk is dat de betrokken persoon niet zal worden aangeworven. (Stel dat de KMO deze informatie toch wil bewaren, dan moet zij de sollicitant hierover informeren en de mogelijkheid geven om zich hiertegen te verzetten);
  - een KMO ontslaat een personeelslid. De KMO mag het personeelsdossier archiveren en bijhouden zolang de verjaringstermijn voor een mogelijke rechtsvordering loopt of de sociale wetgeving dit voorschrijft. Nadien heeft de KMO echter geen reden meer om deze persoonsgegevens nog langer te bewaren en moet zij deze wissen;
  - een headhunter bureau verzamelt CV's van werkzoekenden om deze te koppelen aan een geïnteresseerde werkgever. Het bureau bewaart deze CV's gedurende tien jaar. Deze periode is disproportioneel ten opzichte van het doel dat erin bestaat om op korte termijn een job te vinden voor de werkzoekende.

Voer een bewaarpolitiek in met een gedifferentieerde toegang. De behandeling van lopende dossiers vereist een bewaring waarbij de gegevens normaal beschikbaar en toegankelijk zijn voor de dossierbeheerder. Zodra een dossier kan worden gearchiveerd, moet de KMO kiezen voor een bewaringswijze waarbij de gegevens slechts beperkt beschikbaar en toegankelijk zijn. Die tweede bewaarmethode is verantwoord gelet op doeleinden van de verdere bewaring, zoals de naleving van de wettelijke voorschriften inzake verjaring of verplichte bewaartermijnen. Wanneer ook die bewaring niet langer nuttig is, moeten de gegevens gewist worden.

TO DO

Maak een inventaris van hoelang u al uw persoonsgegevens bewaart en motiveer steeds waarom u die gegevens nog nodig hebt. Voer ook een bewaarpolitiek in met een gedifferentieerde toegang.

Voor meer info

- ❖ Artikel 5.1.e) AVG – Beginselen inzake verwerking van persoonsgegevens

1.6 Transparantie

Zonder noodzakelijke informatie over hun rechten, het hoe en waarom van de verwerkingsactiviteit, kunnen de betrokken en hun rechten niet uitoefenen. Daarom is transparante communicatie cruciaal. Als verwerkingsverantwoordelijke moet de KMO *proactief* communiceren zodat betrokkenen precies weten wie de persoonsgegevens verwerkt, waarom en tot wie zij zich kunnen richten bij problemen.

Transparantie is een overkoepelende verplichting die gevolgen heeft op drie vlakken: Ten eerste heeft de KMO een plicht om de betrokkene proactief te informeren. Ten tweede verplicht transparantie de verwerkingsverantwoordelijke om de uitoefening van de rechten van de betrokkenen te faciliteren (zie verder titel III Rechten van de betrokkene). Tot slot heeft transparantie gevolgen voor *de manier van communiceren*. Als verwerkingsverantwoordelijke rust op de KMO een plicht om alle communicatie over de verwerking van persoonsgegevens op stellen in duidelijke en begrijpelijke bewoordingen die zijn afgestemd op het doelpubliek. Bovendien moet de informatie gemakkelijk toegankelijk zijn. Dit betekent dat het voor de betrokkene onmiddellijk duidelijk moet zijn waar hij of zij de nodige informatie kan vinden.

- o **VOORBEELD**:
  - een privacybeleid op de website van een KMO mag geen overmatig juridische taalgebruik bevatten en onnodig complexe formuleringen gebruiken;
  - de weblink naar het privacybeleid moet duidelijk zichtbaar zijn op de website van de KMO. De kleur en een in het oog springende positie kunnen hiertoe bijdragen;
  - zinnen zoals *"We kunnen uw gegevens gebruiken om nieuwe diensten te ontwikkelen" of "We kunnen uw gegevens gebruiken om gepersonaliseerde diensten aan te bieden"* zijn niet transparant omdat het onduidelijk is welke diensten worden ontwikkeld of wat personaliseren precies inhoudt.

Lees zeker ook titel III.1 Het recht op informatie/de plicht om te informeren om meer informatie te krijgen over transparantie binnen de context van het recht op informatie en de plicht om proactief te informeren bij de inzameling van persoonsgegevens.

TO DO

Zorg ervoor dat je op transparante wijze communiceert naar klanten, personeel en leveranciers over de verwerking van hun persoonsgegevens. Formuleer de informatie in bewoordingen die aangepast zijn aan de doelgroep (bijv. kinderen).

Voor meer info

- ❖ Artikel 5.1.a) AVG – Beginselen inzake verwerking van persoonsgegevens
- ❖ Artikel 12 AVG – Transparante informatie
- ❖ Artikelen 13 en 14 AVG – Te verstrekken informatie
- ❖ Richtlijnen van de WP29 over transparantie onder Verordening 2016/679 – WP260

1.7 Beveiliging

Elke KMO moet passende technische en organisatorische maatregelen nemen om de veiligheid van de persoonsgegevens te garanderen. Deze maatregelen zijn zowel organisatorisch als technisch – een kant-en-klaar beveiligingssoftwarepakket aanschaffen volstaat dus niet altijd! De KMO moet de persoonsgegevens beschermen tegen ongeoorloofde toegang of verwerking, verlies en beschadiging.

De concrete implementatie van deze verplichting kan variëren volgens de risico's en de omvang van die verwerking, de kost en de technische haalbaarheid. De AVG verlangt dus niet noodzakelijk dat een bescheiden KMO het neusje van de zalm aanschaft inzake informatiebeveiliging. Hieronder geven we enkele voorbeelden van organisatorische (1.7.1) en technische beschermingsmaatregelen (1.7.2).

Voor meer info
❖ Artikel 5.1.f) AVG – Beginselen inzake verwerking van persoonsgegevens
❖ Artikel 32 AVG – Beveiliging van de verwerking
❖ Cybersecurity – Gids voor de KMO van het Centre for Cyber Security Belgium
❖ Richtlijnen van ENISA voor KMO's over veilige verwerking van persoonsgegevens

1.7.1 Organisatorische maatregelen

1.7.1.1 Sensibilisering en opleiding

Sensibiliseer het voltallige personeel om hen vertrouwd te maken met de basisbeginselen inzake gegevensbescherming. Met name de personeelsleden met toegang tot de persoonsgegevens zelf moeten opgeleid worden zodat zij die toegang niet (on)bewust misbruiken. Deze laagdrempelige maatregel moet elke KMO invoeren.

1.7.1.2 Stippel een veiligheidsbeleid uit

Dit betekent dat het management van de KMO een uitdrukkelijk beleid uitdenkt en implementeert. Dit beleid omvat op zijn minst de volgende punten:

- procedures in het leven roepen bij aankomst en vertrek van gebruikers;
- het verspreiden van een algemene gedragscode voor het ICT-gebruik;
- het aanduiden van een verantwoordelijke voor informatiebeveiliging;
- het regelmatig plannen en getrouw uitvoeren van veiligheidsaudits;
- een toegangsbeleid uitdenken dat uitsluitend toegang verleent tot persoonsgegevens op een "need-to-know"-basis;
- het opstellen van interne procedures om klachten te behandelen en adequaat te reageren op incidenten (bijv. gegevenslek).

1.7.2 Technische maatregelen

Een aantal laagdrempelige maatregelen kunnen eenvoudig worden uitgerold in de IT-infrastructuur van de meeste KMO's, zoals:

- gebruik een virusscanner en update deze systematisch en tijdig;
- maak systematisch een back-up om te beschermen tegen verlies;
- update systematisch en automatisch al uw softwareprogramma's;
- laat uw website functioneren via een beveiligde Https-verbinding;
- installeer een "firewall"(zowel hard- als software);
- garandeer de fysieke veiligheid van servers door alleen geautoriseerd personeel hier toe te laten (bv. aan de hand van badges);
- voer een toegangssysteem in met een uniek identificatiemiddel (login) voor elke gebruiker met een authenticatiemechanisme.

2 Beschermingsmaatregelen afgestemd op de risico's

De AVG stelt de rechten van de betrokkene centraal en wil daarom de risico's waarmee een verwerking gepaard gaat, identificeren en inperken. De AVG zet de KMO op weg om die noodzakelijke risicoanalyse door te voeren en reikt een aantal middelen aan om dit proces te vergemakkelijken. Bovendien helpen deze maatregelen om de naleving van de AVG proactief te garanderen. In dit hoofdstuk doorlopen we de volgende stappen:

- Stap 1 : het register van de verwerkingsactiviteiten – breng verwerkingen in kaart;
- Stap 2 : duid een functionaris voor de gegevensbescherming (DPO) aan;
- Stap 3 : voer een gegevensbeschermingseffectbeoordeling (GEB) uit;

Stappen 2 en 3 hoeft een KMO slechts te nemen indien aan bepaalde voorwaarden is voldaan. In geval van twijfel doet de KMO er goed aan om te documenteren waarom zij van mening was dat die stappen niet noodzakelijk waren.

2.1 Stap 1: Maak een overzicht met het register van de verwerkingsactiviteiten

Het opstellen van een overzicht van alle verwerkingen van persoonsgegevens is een onmisbare stap in de beoordeling van het risico. De AVG verplicht iedere verwerkingsverantwoordelijke en verwerker om een interne documentatie bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Met dit register krijgen zij inzicht in de verwerkingen die zij verrichten. Dit register moet schriftelijk (elektronisch of op papier), helder en begrijpelijk zijn.

Het register bevat een overzicht van de verwerkingsactiviteiten en niet van de persoonsgegevens zelf. Het register moet op zijn minst de volgende informatie vermelden:

- ***Wie***: naam en contactinformatie van de verwerkingsverantwoordelijke en functionaris (DPO);
- ***Waarom***: per verwerking vermeldt het register in detail de verwerkingsdoeleinden;
- ***Wat***: per verwerking vermeldt het register de soorten van persoonsgegevens en betrokkenen;
- ***Waar***: het register vermeldt alle ontvangers van de persoonsgegevens, de doorgiftes naar een land buiten de Europese Unie en de eventuele passende waarborgen voor zo een doorgifte;
- ***Bewaartermijn***: indien mogelijk, de termijn waarbinnen men persoonsgegevens moet wissen;
- ***Beveiliging***: indien mogelijk, een algemene beschrijving van de beveiligingsmaatregelen.

Het register vervult een cruciale rol in de naleving van de AVG. Het is een basisinstrument om tal van andere plichten te kunnen vervullen zoals het informeren van betrokkenen en het efficiënt omgaan met verzoeken om hun rechten uit te oefenen (zoals inzage, verbetering en uitwissing). Toch voorziet de AVG in een uitzondering voor KMO's. De draagwijdte van deze uitzondering is echter zeer beperkt:

- een organisatie met minder dan 250 personen in dienst moet geen register houden;
- *tenzij*:
  - de verwerking van persoonsgegevens niet incidenteel is; *of*
  - de verwerking een risico inhoudt voor de rechten en vrijheden van de betrokkenen; *of*
  - de verwerking betrekking heeft op gevoelige gegevens.

Hieronder volgt een korte verduidelijking van deze situaties waarin een KMO toch een register moet bijhouden:

- **als de verwerking gewoonlijk (niet incidenteel) is**: incidenteel betekent dat de verwerking van persoonsgegevens niet systematisch plaatsvindt binnen de KMO. Indien de verwerking ingebed is in het normale functioneren van de KMO zal de KMO, minstens voor deze verwerking, een register moeten bijhouden. Binnen een KMO zijn bijvoorbeeld de verwerkingen die verband houden met klanten-, personeels- (human resources) en leveranciersbeheer niet incidenteel.

  - **VOORBEELD**: Een loodgietersbedrijf met twintig personeelsleden moet een register bijhouden voor de verwerkingen van persoonsgegevens van haar klanten, personeel en leveranciers (voor zover het niet gaat om een rechtspersoon in dit laatste geval).

- **de verwerking houdt een risico in voor de rechten en vrijheden van de betrokkenen**: dit is een catch-all bepaling die een omzeiling van de risico-gebaseerde aanpak wil voorkomen. Overweging 75 van de AVG somt enkele situaties op waarin sprake is van een dergelijk risico: het toebrengen van een financieel of maatschappelijk nadeel, profilering, de onmogelijkheid voor de betrokkene om zijn of haar rechten uit te oefenen, de hoeveelheid van persoonsgegevens, het aantal betrokkenen en de verwerking van gegevens van kwetsbare personen (bv. kinderen).

  - **VOORBEELD**: Een kinderdagverblijf dat gegevens van de opgevangen kinderen registreert, moet hiervoor een register aanleggen.

- **de verwerking van gevoelige gegevens**: de verwerking van bepaalde gevoelige gegevens brengt een hoger risico op later misbruik met zich mee.

  - **VOORBEELD**: Een huisartsenpraktijk, die medische gegevens verwerkt van haar patiënten moet een register aanleggen.

Kort samengevat betekent dit dat de verplichting tot het houden van een register slechts in een heel beperkt aantal situaties wegvalt. Daarom raden we alle verwerkingsverantwoordelijken en verwerkers aan om altijd een register te houden, zelfs al zou dit strikt genomen niet verplicht zijn. Voor een KMO met een beperkt aantal gegevensverwerkingen is dit geen onoverkomelijke taak. Bovendien is het opstellen van dit register onontbeerlijk om een correcte inschatting te maken van de verplichtingen die voortvloeien uit de AVG.

We moedigen sectorfederaties aan om templates uit te werken met gemeenschappelijke elementen die KMO's kunnen overnemen in hun register.

TO DO

Stel een register van de verwerkingsactiviteiten op – u kan hiervoor gebruik maken van de volgende hulpmiddelen:
1) het model van register opgesteld door de Privacycommissie; en
2) de toelichting bij de voorafgaande aangifte die de Privacycommissie heeft uitgewerkt. Hoewel de verplichting tot voorafgaande aangifte wegvalt, bevat deze aangifte veel nuttige informatie die ook in het register moet voorkomen. Deze toelichting bevat een lijst van veelvoorkomende doeleinden die de KMO kan helpen bij het invullen van hun register.

Voor meer info

- Artikel 30 AVG – Register van de verwerkingsactiviteiten
- Aanbeveling 06/2017 van de Privacycommissie over het register
- Schema van de Privacycommissie: "Moet ik een register bijhouden?"
- FAQ van de Privacycommissie over het register van de verwerkingsactiviteiten

2.2 Stap 2: Duid een functionaris voor de gegevensbescherming (DPO) aan

Sommige verwerkingsverantwoordelijken en verwerkers moeten een functionaris voor gegevens-bescherming (data protection officer of DPO) aanduiden. De functionaris heeft als taak om:

- te informeren en te adviseren om de AVG na te leven;
- op vraag advies te verlenen met betrekking tot de GEB;
- te controleren of verwerkingen de AVG respecteren;
- op te treden als contactpunt voor de toezichthoudende autoriteit.

2.2.1 Moet ik een functionaris voor gegevensbescherming aanstellen?

Niet iedere KMO moet een functionaris voor gegevensbescherming aanduiden. De aanduiding is **verplicht** in drie gevallen:

- een overheidsinstantie verricht de verwerking; of
- de KMO is *hoofdzakelijk* belast met *grootschalige*, regelmatige en stelselmatige observatie van natuurlijke personen; of
    - **VOORBEELD**: geolokalisatie via een mobiele app, profilering en observatie door middel van bewakingscamera's zijn mogelijke voorbeelden van stelselmatige observatie.
- de KMO is *hoofdzakelijk* belast met *grootschalige* verwerking van gevoelige gegevens.

De begrippen "*hoofdzakelijk*" en "*grootschalig*" zijn cruciaal om te bepalen of een KMO een DPO moet aanstellen. Hoofdzakelijk betekent dat de verwerking voortvloeit uit de hoofdactiviteiten van de KMO en niet uit een louter ondersteunende nevenactiviteit zoals het uitbetalen van personeel of IT support. Grootschaligheid kan zowel slaan op het volume van de gegevens, het aantal betrokkenen, de duurtijd als de geografische dekking en laat zich niet zomaar herleiden tot een welbepaald cijfer.

- **VOORBEELD:**
    - een KMO verzamelt en combineert als hoofdactiviteit persoonsgegevens uit verschillende bronnen, om klantenprofielen op te stellen en nadien door te verkopen aan adverteerders. Deze profilering is een vorm van stelselmatige observatie. Tot slot zal *in concreto* moeten beoordeeld worden of de verwerking grootschalig is of niet. Zo ja, is de aanduiding van een DPO noodzakelijk;
    - een KMO installeert één bewakingscamera die gericht is op de kassa van de winkel. Het filmen leidt tot een stelselmatige observatie van natuurlijke personen. De verwerking is echter niet grootschalig en het filmen voor veiligheidsdoeleinden is geen hoofdactiviteit van de KMO. In dit geval hoeft de KMO geen DPO aan te duiden;
    - een KMO beheert een website waarmee ziekenhuizen met huisartsen uit de hele provincie medische informatie kunnen uitwisselen. De hoofdactiviteit van de KMO bestaat in het uitwisselen van gevoelig gegevens. De regionale ontplooiing van deze website is voldoende grootschalig om de aanduiding van een DPO te verplichten.

U mag trouwens altijd **vrijwillig** een functionaris voor gegevensbescherming aanduiden, zelfs als dit juridisch niet verplicht is. Opgepast: Indien u vrijwillig een functionaris voor gegevensbescherming aanduidt, moet u alle regels naleven van de AVG over de taken en de positie van de functionaris. Let dus op met een lichtzinnig gebruik van de functietitel DPO of functionaris! Gebruik deze titel alleen als het gaat om een échte functionaris voor gegevensbescherming in de zin van de AVG.

2.2.2 Positie van de functionaris voor gegevensbescherming

De KMO moet de functionaris voor gegevensbescherming ondersteunen door toegang te verlenen tot persoonsgegevens en verwerkingen. Ook moeten de nodige middelen ter beschikking gesteld worden voor het vervullen van zijn taken (tijd, training, faciliteiten en financieel). De functionaris moet toegang hebben tot het hoge management om problemen aan te kaarten.

De functionaris voor gegevensbescherming moet ook onafhankelijk zijn. Dit betekent dat de KMO:

- de functionaris geen instructies mag geven over de uitvoering van zijn/haar taken;
- de functionaris niet mag straffen of ontslaan voor de uitvoering van zijn/haar taken;

Om de onafhankelijkheid te waarborgen mag de functionaris voor gegevensbescherming slechts andere taken of functies opnemen indien die bijkomende verantwoordelijkheden niet leiden tot een belangenconflict. Dit houdt in dat de functionaris geen positie mag hebben waarin hij/zij het doel en de middelen van de verwerking van persoonsgegevens bepaalt. Conflicterende functies omvatten vooral directieposten (hoofd HR, hoofd IT, gedelegeerd bestuurder) maar kunnen ook slaan op lagere functies.

De AVG voorziet in de mogelijkheid om een externe functionaris voor gegevensbescherming aan te wijzen in het raam van een dienstverleningscontract.

TO DO

1) Ga na of u een functionaris voor gegevensbescherming moet aanduiden en **documenteer** bij twijfel waarom u wel/niet een DPO aanstelt.
2) Ga na of uw functionaris voor gegevensbescherming geen andere taken opneemt die de onafhankelijkheid van zijn/haar positie ondermijnen (belangenconflict).
3) Zelfs als u geen echte DPO aanstelt, raden we aan om een persoon aan te duiden die de naleving van de AVG controleert en optreedt als contactpersoon voor betrokkenen die hun rechten uitoefenen. Geef deze persoon niet de titel 'DPO' of 'functionaris voor de gegevensbescherming'!

Voor meer info

- Artikel 37-39 AVG – Functionaris voor gegevensbescherming
- Richtlijnen van de WP 29 voor de functionarissen voor gegevensbescherming – WP243
- Aanbeveling 04/2017 van de Privacycommissie m.b.t. functionaris voor gegevensbescherming
- Schema van de Privacycommissie: "Moet ik een DPO aanstellen?"
- FAQ van de Privacycommissie over de functionaris voor gegevensbescherming

2.3 Stap 3: Voer een gegevensbeschermingseffectbeoordeling uit (GEB)

De GEB is een voortdurend proces dat dient om risico's voor de rechten en vrijheden van natuurlijke personen te detecteren, evalueren en uiteindelijk te beheersen. De GEB is uitsluitend verplicht wanneer de verwerking een **hoog risico** inhoudt voor de rechten en vrijheden van natuurlijke personen. De WP29 heeft een lijst van een negental factoren opgesteld die helpen om te beoordelen wanneer er een hoog risico is (zie bij meer info). Hoe meer factoren aanwezig zijn in de verwerking, des te groter de kans dat er sprake is van een hoog verwerkingsrisico. U moet geval per geval beoordelen of het risico hoog en een GEB dus noodzakelijk is.

De KMO moet de GEB uitvoeren voor de verwerking begint en moet nadien deze evaluatie op gezette tijdstippen overdoen zodat de risicobeoordeling en de bijhorende maatregelen up-to-date blijven. Een GEB omvat ten minste:

- een gedetailleerde en duidelijke beschrijving van de verwerkingen en de doeleinden;
- een beoordeling van de proportionaliteit van de verwerkingen t.o.v. die doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om die risico's aan te pakken.

- **VOORBEELD:**
  - een KMO observeert het surfgedrag van haar personeel om overmatig privégebruik tijdens de werkuren te voorkomen. Er is sprake van stelselmatige observatie en een evaluatie. Bovendien bevinden de werknemers zich in een ondergeschikte – dus kwetsbare – positie ten aanzien van de werkgever. Het risico is in dit geval hoog en een GEB is hoogst waarschijnlijk noodzakelijk.

De GBA zal in de toekomst ook een lijst opstellen van soorten verwerkingen waarvoor een GEB automatisch verplicht is. In een aantal gevallen vindt de AVG zelf dat het risico per definitie hoog is en moet u sowieso een GEB uitvoeren:

- **bij een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, waaronder profilering,** indien dit leidt tot beslissingen die de betrokkene aanzienlijk treffen;
  - **VOORBEELD**: De KMO maakt gebruik van een online wervingsplatform dat op basis van een automatische lezing van het CV, kandidaten automatisch selecteert of afwijst.
- **bij de grootschalige** verwerking van **gevoelige persoonsgegevens** in de zin van artikel 9 en 10 AVG;
  - **VOORBEELD**: een start-up ontwikkelt een health-app op basis van een open platform (bijv. Android) dat gegevens over slaap, eetgewoonten en fysieke activiteit verzamelt.
- bij de stelselmatige en grootschalige **monitoring** van openbaar toegankelijke ruimten.

Soms volstaan de maatregelen die u neemt in het kader van de GEB niet om het hoge risico voldoende in te perken. Indien na het uitvoeren van de GEB het residuele risico – dit is het risico dat overblijft ondanks de maatregelen die u neemt in het kader van de GEB – nog steeds hoog blijft, moet u het advies van de GBA inwinnen.

TO DO

Beoordeel de noodzaak tot het uitvoeren van een GEB:
1) bevindt u zich in een van de drie gevallen die een GEB vereisen?
2) indien niet: voert de KMO verwerkingen uit die een hoog risico kunnen vormen voor de rechten en vrijheden van natuurlijke personen?
3) indien niet: een GEB is niet nodig maar de KMO zal haar **beslissing moeten rechtvaardigen en documenteren**.

Voor meer info

- Artikel 35-36 AVG – Gegevensbeschermingseffectbeoordeling
- Richtsnoeren van de WP29 voor Gegevensbeschermingseffectbeoordeling – WP248
- Aanbeveling van de Privacycommissie de gegevensbeschermingseffectbeoordeling
- Schema van de Privacycommissie: “Moet ik een GEB uitvoeren?”
- FAQ van de Privacycommissie over de gegevensbeschermingseffectbeoordeling

3 Externe dienstverleners

Om kosten te besparen op de installatie van een autonome IT-infrastructuur doen KMO’s vaak beroep op externe dienstverleners – verwerkers dus – om persoonsgegevens op te slaan of bepaalde diensten te bekomen (outsourcing).

- **VOORBEELD**: de lokale brouwerij doet beroep op een sociaal secretariaat om de loonadministratie te beheren. De brouwerij communiceert de details van de betaling zoals het tijdstip, loonstijgingen of een ontslag. Het sociaal secretariaat gebruikt haar eigen IT-infrastructuur om de personeels-gegevens op te slaan en de loonadministratie waar te nemen. Het sociaal secretariaat is de verwerker en de brouwerij is verwerkingsverantwoordelijke.

Beroep doen op een externe dienstverlener is toegelaten, maar moet steeds gepaard gaan met een aantal waarborgen. Deze waarborgen moeten er voor zorgen dat de KMO voldoende controle behoudt over wat er met de persoonsgegevens gebeurt en dat deze behoorlijk beveiligd blijven. Het opslaan en verwerken van gegevens in de Cloud is een courante vorm van outsourcing. De KMO zal in de keuze van de Cloud Service Provider (CSP) rekening moeten houden met o.a. de veiligheid van de uitgewisselde persoonsgegevens. Het machtsonevenwicht in de contractuele relatie ontslaat de KMO niet van haar verantwoordelijkheid om alleen contractuele voorwaarden te aanvaarden die in overeenstemming zijn met de AVG.

Hieronder volgen de maatregelen die u moet nemen indien u beroep doet op een externe verwerker:

3.1 Sluit een contract af

3.1.1 Selecteer zorgvuldig

KMO's mogen uitsluitend beroep doen op verwerkers die *afdoende garanties* bieden opdat de verwerking aan de vereisten van de AVG zou voldoen en de rechten van de betrokkene gewaarborgd blijven. De garanties moeten onder meer betrekking te hebben op de beveiliging en het toepassen van *passende technische en organisatorische* maatregelen (zie met name II.1.7 Beveiliging).

3.1.2 Sluit een schriftelijke overeenkomst af

Wanneer de verwerking van persoonsgegevens aan een verwerker wordt toevertrouwd, moeten beide partijen een "verwerkersovereenkomst" afsluiten. Dit contract moet uitdrukkelijk bepalen dat de dienstverlener de persoonsgegevens *uitsluitend op basis van de schriftelijke instructies* van de KMO mag verwerken. De overeenkomst moet zeker de volgende elementen bevatten:

- onderwerp en duur van de overeenkomst, de doeleinden en aard van de verwerking, het soort gegevens, de categorieën van betrokkenen en de rechten en verplichtingen van beide partijen;
- de verwerker garandeert dat hij de persoonsgegevens enkel op basis van de schriftelijke instructies van de KMO zal verwerken en niet voor enige andere doeleinde zal aanwenden (behoudens een uitdrukkelijke wettelijke verplichting);
- de verwerker garandeert om passende technische en organisatorische maatregelen te zullen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- de verwerker belooft geen andere verwerker (onderaannemer) in dienst te nemen zonder voorafgaande schriftelijke toestemming van de KMO. Als de verwerker toch een onderaannemer inschakelt moet de verwerker alle verplichtingen opleggen aan de onderaannemer die voort-vloeien uit de eerste verwerkingsovereenkomst tussen de KMO en de eerste verwerker;
- de verwerker waarborgt dat personen die door hem gemachtigd zijn tot het verwerken van de persoonsgegevens (bijv. technici belast met het beheer van de dienst) zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- de verwerker gaat akkoord om de KMO voor zover mogelijk bijstand te verlenen bij het vervullen van diens plicht om aan de verzoeken om uitoefening van de rechten van de betrokkenen te beantwoorden;
- de verwerker verklaart zich bereid om, waar passend, aan de KMO bijstand te verlenen bij het doen nakomen van haar verplichtingen wat betreft beveiliging, melding en/of mededeling van een inbreuk in verband met persoonsgegevens of een GEB;
- de gegevens worden niet buiten de Europese Unie doorgegeven naar bestemmingen die geen adequaat beschermingsniveau bieden of zonder bijkomende passende waarborgen die eerst met de KMO zullen worden afgesproken;
- de verwerker waarborgt dat na afloop van de dienstverlening alle persoonsgegevens veilig gewist of aan de KMO terugbezorgd zullen worden, en bestaande kopieën verwijderd zullen worden;
- de verwerker gaat akkoord om aan de KMO alle informatie ter beschikking te stellen die nodig is om de nakoming van diens verplichtingen aan te tonen en audits, waaronder inspecties, door de KMO of een door de KMO gemachtigde controleur mogelijk te maken en eraan bij te dragen.

3.1.3 Controleer de naleving van de afspraken

De KMO moet erover waken dat de externe dienstverlener de gemaakte afspraken daadwerkelijk naleeft. Vandaar dat de verwerkersovereenkomst ook dient te bepalen dat de dienstverlener aan de KMO alle informatie ter beschikking moet stellen die nodig is om de nakoming van diens verplichtingen aan te tonen.

TO DO

1) Beoordeel huidige en toekomstige contracten met externe dienstverleners en breng tijdig (dus vóór 25 mei 2018) de nodige veranderingen aan. Hou daarbij rekening met de minimale elementen die artikel 28 AVG voorschrijft, waaronder de verbintenis dat de toevertrouwde persoonsgegevens uitsluitend op basis van de schriftelijke instructies van de KMO mogen worden verwerkt;
2) Verifieer dat zowel huidige als toekomstige dienstverleners afdoende waarborgen bieden, in het bijzonder wat betreft de beveiliging van persoonsgegevens;
3) Vraag op gepaste tijdstippen de nodige informatie op die aantoont dat de dienstverlener zijn verplichtingen nakomt.

Voor meer info

- Artikel 28 AVG – Verwerker
- Artikel 29 AVG – Verwerking onder gezag van de verwerkingsverantwoordelijke of verwerker
- Advies 05/2012 van de WP29 over Cloud Computing – WP196
- Advies 10/2016 van de Privacycommissie over de gebruikmaking van cloudcomputing door de verantwoordelijke voor de verwerking

4 Waar gaan uw gegevens naar toe?

Soms verkrijgt een KMO persoonsgegevens in België, maar doet zij voor de verdere verwerking hiervan beroep op de diensten van een verwerker waarvan de servers zich bevinden in het buitenland. Binnen de Europese Unie mogen alle persoonsgegevens vrij circuleren. Als de gegevensverwerking plaatsvindt in bijvoorbeeld Duitsland, dan hoeft de KMO geen extra waarborgen te eisen. Vindt de gegevens-verwerking plaats buiten de Europese Unie dan mag de doorgifte van de persoonsgegevens slechts plaatsvinden onder strikte voorwaarden.

De doorgifte naar een "derde land" buiten de Europese Unie is toegelaten:

- wanneer deze bestemming door de Europese Commissie erkend is als een bestemming met een gelijkaardig beschermingsniveau (een adequaatheidsbesluit). De lijst van erkende bestemmingen kan u terug vinden op deze website;
- wanneer de verwerker in de overeenkomst bijkomende passende waarborgen biedt om een gelijkaardig beschermingsniveau op contractuele wijze tot stand te brengen. Dit kan door modelbepalingen toe te voegen die de Europese Commissie of de GBA heeft goedgekeurd;

Deze mechanismen garanderen de veiligheid van de persoonsgegevens en zorgen ervoor dat betrokkenen hun rechten kunnen uitoefenen, ook al vindt de verwerking plaats in een land met andere soort privacywetgeving.

De AVG voorziet nog in enkele andere mechanismen om doorgiftes naar een derde land toe te laten (bindende bedrijfsvoorschriften, gedragscodes, afwijkingen voor specifieke situaties etc.…). Deze gaan echter het bestek van deze brochure te buiten. Het is vooral van belang dat een KMO weet waar haar gegevens naartoe gaan en beseft dat een doorgifte buiten de Europese Unie extra waarborgen vereist.

- **VOORBEELD**: een KMO doet beroep op een Zwitserse verwerker om het e-mail-verkeer te beheren (e-mailadressen leveren, opslag van e-mails, etc.…). De verwerker bewaart de e-mails op servers die in Zwitserland staan. Deze doorgifte van persoonsgegevens vereist geen bijkomende waarborgen omdat Zwitserland door de Europese Commissie is erkend als een bestemming met een gelijkaardig beschermingsniveau.

TO DO

Controleer of uw verwerker de persoonsgegevens buiten de Europese Unie verwerkt.
1) Zo ja, controleer dan of deze bestemming is opgenomen in de lijst van bestemmingen met een adequaat beschermingsniveau die door de Europese Commissie zijn erkend.
2) Staat de bestemming niet op deze lijst, dan moet u extra contractuele waarborgen onderhandelen.

Voor meer info

- Hoofdstuk V AVG – Doorgiften van persoonsgegevens aan derde landen
- Webpagina van de Europese Commissie voor "Data transfers outside the EU"

III. Rechten van de betrokkene

Naast het opleggen van bepaalde verplichtingen die hierboven werden besproken, voorziet de AVG in rechten die iedere betrokkene kan uitoefenen. De betrokkene oefent deze rechten uit *ten aanzien van de verwerkingsverantwoordelijke*. De verwerker, moet de verwerkingsverantwoordelijke bijstaan om de uitoefening van deze rechten mogelijk te maken. Het gaat in het bijzonder om:

1. het recht op informatie/de plicht om te informeren
2. het recht van inzage
3. het recht op verbetering
4. het recht op gegevenswissing
5. het recht op beperking van de gegevensverwerking
6. het recht van bezwaar
7. het recht op gegevensoverdraagbaarheid
8. het recht om niet aan geautomatiseerde individuele besluitvorming onderworpen te worden

Let op: sommige rechten gelden niet voor elke rechtsgrond (zie II.1.1 Rechtsgrond)! Bij de bespreking van ieder recht lichten we steeds het verband tussen de rechtsgrond en het recht verder toe.

In de uitoefening van de rechten van de betrokkenen speelt transparantie ook een sleutelrol. Zo moet de verwerkingsverantwoordelijke:

- de betrokkene duidelijk informeren over bestaan van deze rechten (III.1 Informatie);
- in begrijpelijke en heldere taal communiceren als een betrokkene rechten uitoefent;
- de uitoefening van deze rechten faciliteren, onder meer d.m.v. elektronische middelen;

o **VOORBEELD**: plaats op uw website een online formulier om het recht op toegang uit te oefenen.

De KMO mag **geen betaling** vragen voor het uitoefenen van deze rechten. U mag wel een vergoeding aanrekenen als het verzoek van de betrokkene duidelijk ongegrond of buitensporig is. De vergoeding moet afgestemd zijn op de administratieve kost voor de KMO om gevolg te geven aan het verzoek. U moet natuurlijk kunnen aantonen dat het verzoek duidelijk ongegrond of buitensporig is.

Wanneer de betrokkene één van haar rechten uitoefent, moet de KMO hier **binnen één maand** op reageren. Gaat het om een complex verzoek, dan kan de KMO de termijn met twee maanden verlengen nadat de betrokkene hier binnen één maand van op de hoogte is gebracht. Als de KMO kan aantonen dat het verzoek duidelijk ongegrond of buitensporig is, mag zij het verzoek negeren.

o **VOORBEELD**: een klant bestookt een KMO wekelijks met tientallen verzoeken tot uitoefening van zijn recht op inzage, zonder gegronde reden. De KMO mag het verzoek negeren of een vergoeding aanrekenen die overeenstemt met de administratieve kost van het bezorgen van een antwoord.

Wanneer de KMO geen gevolg geeft aan het concrete verzoek van de betrokkene, moet zij één maand na ontvangst van het verzoek meedelen waarom het verzoek zonder gevolg blijft (bijv. waarom ze een gegevenswissing niet doorvoert). Bovendien moet de KMO betrokkene wijzen op de mogelijkheid om klacht neer te leggen bij de GBA of beroep in te stellen bij een rechter.

TO DO

Werk een interne procedure uit en duid een centrale contactpersoon aan die binnen één maand gevolg kan geven aan een verzoek van de betrokkenen tot uitoefening van zijn/haar rechten.

Voor meer info

- ❖ Artikel 12 AVG – Nadere regels voor de uitoefening van de rechten van de betrokkene
- ❖ Richtlijnen van de WP29 over transparantie onder Verordening 2016/679 – WP260

1 Het recht op informatie/de plicht om te informeren

Elke betrokkene heeft recht op bepaalde informatie wanneer een KMO gegevens verwerkt die op hem of haar betrekking hebben. De KMO heeft een plicht om de betrokkene te informeren. De AVG maakt een onderscheid tussen de rechtstreekse inzameling van persoonsgegevens bij de betrokkene zelf (rechtstreekse inzameling – artikel 13 AVG) en de situatie waarbij de persoonsgegevens niet bij de betrokkene zelf maar uit een andere bron zijn verkregen (onrechtstreekse inzameling – artikel 14 AVG).

1.1 Welke informatie?

Zowel bij de rechtstreekse als onrechtstreekse inzameling van persoonsgegevens moet een KMO als verwerkingsverantwoordelijke bepaalde informatie verstrekken aan de betrokkene. Hier overlopen we de basisinformatie die u bij rechtstreekse dan wel onrechtstreekse inzameling aan de betrokkene moet meedelen:

Informatie	Rechtstreeks	Onrechtstreeks
doeleinden en rechtsgrond van de verwerking	✓	✓
identiteit en contactgegevens van de verwerkings-verantwoordelijke en de DPO (als er een DPO is)	✓	✓
de ontvangers of categorieën ontvangers van de gegevens	✓	✓
bij doorgifte buiten de EU: het bestaan van een adequaatheids-besluit of passende waarborgen en hoe u hiervan een kopie kan krijgen	✓	✓
uitleg over het gerechtvaardigde belang van de verwerkings-verantwoordelijke als de verwerking steunt op deze rechtsgrond	✓	
de categorieën van verwerkte gegevens		✓

Bovendien schrijft de AVG voor dat een KMO de onderstaande informatie moet verstrekken om een behoorlijke en transparante verwerking te waarborgen. De richtlijnen van de WP29 over transparantie leggen wanneer u deze informatie moet meedelen.

Informatie	Rechtstreeks	Onrechtstreeks
de bewaartermijn, of indien onmogelijk, de criteria om die termijn te bepalen	✓	✓
het recht op toegang, uitwissing, verbetering, beperking, bezwaar en overdraagbaarheid	✓	✓
het recht om een klacht in te dienen bij een toezichthoudende autoriteit	✓	✓
steunt de verwerking op toestemming: het recht om de toestemming te allen tijde in te trekken	✓	✓
het bestaan van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica hiervan en de verwachte gevolgen van die verwerking voor de betrokkene	✓	✓
uitleg over het gerechtvaardigde belang van de verwerkings-verantwoordelijke als de verwerking steunt op deze rechtsgrond		✓
de bron van de gegevens		✓
of de betrokkene verplicht is de persoonsgegevens te verstrekken (door de wet of een contract) en wat de gevolgen zijn bij een weigering om die gegevens te verstrekken	✓	

De verwerkingsverantwoordelijke moet de bovenstaande informatie uit deze tweede tabel opnieuw meedelen bij een verdere verwerking voor een nieuw maar verenigbaar doeleinde dat afwijkt van het oorspronkelijk doeleinde (zie titel II.1.2 Doeleinde). In dit geval moet de KMO de betrokkene ook informatie geven over de analyse die aantoont dat het nieuwe en oude doeleinde verenigbaar zijn.

1.2 Wanneer moet de informatie worden verstrekt?

Bij de rechtstreekse inzameling moet de KMO de informatie meedelen op het moment van inzameling van de persoonsgegevens. Bij de onrechtstreekse inzameling van persoonsgegevens moet de KMO de informatie geven ten laatste binnen één maand na de initiële verkrijging van de persoonsgegevens. Die maximale termijn van één maand wordt ingekort – nooit verlengd – :

- indien de persoonsgegevens worden gebruikt voor communicatie met de betrokkene. De KMO informeert dan uiterlijk op het moment van eerste contact met de betrokkene;
- indien de gegevens aan een andere ontvanger worden doorgegeven. De KMO informeert dan uiterlijk op het tijdstip van de doorgifte van de persoonsgegevens.

Voor de duidelijkheid: als de doorgifte of het eerste contact later plaatsvindt dan één maand na de initiële verkrijging van de persoonsgegevens, moet de KMO de informatie gewoon binnen de maand na de initiële verkrijging meedelen.

Bij elke latere wijziging aan de verwerking (bijv. nieuw ontvangers, verenigbaar doeleinde, doorgifte buiten de EU, etc.…) moet de KMO de betrokkene hier ruim op voorhand over informeren. Des te ingrijpender de wijziging, des te vroeger moet de KMO de betrokkene hiervan op de hoogte stellen zodat deze een redelijk termijn heeft om de impact ervan te appreciëren en zijn/haar rechten uit te oefenen.

1.3 Wanneer moet de KMO geen informatie meedelen?

De KMO moet de informatie niet meedelen indien de betrokkene deze al ontving. Bij onrechtstreekse inzameling van persoonsgegevens gelden bijkomende uitzonderingen. De mededeling van informatie is dan niet noodzakelijk indien:

- het verstrekken van die informatie onmogelijk is of onevenredig veel inspanning vergt. De lat voor deze uitzondering ligt echter zeer hoog waardoor een verwerkingsverantwoordelijke slechts uitzonderlijk deze situaties kan inroepen; *of*
- het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven door de wet; *of*
    - **VOORBEELD**: de wet verplicht de fiscus om bepaalde informatie over een werknemer op te vragen bij de werkgever. De fiscus hoeft de werknemer zelf niet te informeren. De werkgever zal in het kader van zijn plicht om te informeren de werknemer wel op de hoogte stellen van het feit dat de fiscus één van de ontvangers is van de persoons-gegevens.
- de persoonsgegevens vertrouwelijk moeten blijven door een wettelijk beroepsgeheim.

1.4 Hoe moet de informatie worden verstrekt?

We raden aan **om informatie te verstrekken in lagen**. Op die manier vermijdt u dat een teveel aan informatie de transparantie schaadt en de betrokkene verdrinkt in een overvloed van informatie. De gelaagde verstrekking van de informatie verzoent de vereiste van beknoptheid met de vereiste om alle noodzakelijke informatie te verstrekken. Dit vereenvoudigt niet alleen de taak van de verwerkings-verantwoordelijke, maar stelt ook de betrokkene in staat om snel en efficiënt de kerninformatie op te nemen. Om te waken over een eerlijke informatieverstrekking zou de voorstelling van deze informatie er als volgt uit kunnen zien:

- een eerste laag met *basisinformatie*.
    - WAT?: de KMO verstrekt een samenvatting van noodzakelijke basisinformatie die de betrokkene nodig heeft om de impact en draagwijdte van de verwerking in te schatten (bijvoorbeeld: de identiteit van de verwerkingsverantwoordelijke, de doeleinden, de categorieën ontvangers, de bron van de gegevens…).
    - HOE?: in tabelformaat op een duidelijk zichtbare plaats met als titel “Basisinformatie gegevensbescherming” of pop-ups die de toelichting geven tijdens het verzamelen van de persoonsgegevens. Steunt de verwerking op toestemming dan vermeldt u die info best op de plaats waar de betrokkene het akkoord moet geven (bij de ‘akkoord’-knop).
- een tweede laag met gedetailleerde, *bijkomende informatie*.
    - WAT?: dit deel presenteert op een begrijpelijke en overzichtelijke manier de overige informatie die de KMO krachtens artikel 13 en artikel 14 AVG moet meedelen.

- HOE?:de bijkomende informatie kan op verschillende manieren worden verstrekt bijv. via hyperlinks die vertrekken vanuit de basisinformatie of een download via een URL. De bijkomende informatie moet een balans vinden tussen beknoptheid en precisie. De informatie moet gestructureerd zijn zodat deze makkelijk leesbaar is.

TO DO

Pas uw website, app en algemene voorwaarden aan zodat:
1) uw privacybeleid steeds duidelijk zichtbaar is en alle informatie vermeldt van artikel 13/14 van de AVG;
2) uw registratie- en transactiewebpagina's op een gelaagde wijze leiden naar alle informatie van artikel 13/14 van de AVG.

Voor meer info

- Artikel 13 AVG – Rechtstreekse inzameling
- Artikel 14 AVG – Onrechtstreekse inzameling
- Richtlijnen van de WP29 over transparantie onder Verordening 2016/679 – WP260

2 Het recht van inzage

Het recht op inzage stelt de betrokkene in staat om de rechtmatigheid van elke verwerkingsactiviteit te controleren. Het recht op inzage is drieledig:

1) De betrokkene heeft het recht om te weten of de KMO al dan niet zijn of haar persoonsgegevens verwerkt.

2) Zo ja, heeft de betrokkene het recht om de onderstaande informatie te verkrijgen:

- de *doeleinden* van de verwerking;
- de *categorieën van persoonsgegevens*;
- de *ontvangers of categorieën van ontvangers* van de persoonsgegevens;
- de *bewaartermijn* van de persoonsgegevens of de criteria om die termijn te bepalen;
- het *recht* op de gegevenswissing, verbetering van persoonsgegevens en het recht om de verwerking te beperken of hiertegen bezwaar te maken;
- het recht een *klacht* in te dienen bij een toezichthoudende autoriteit;
- de *bron* van de gegevens (bij onrechtstreekse inzameling);
- bij doorgifte *buiten de EU*: de passende waarborgen (bijv. modelbepalingen- zie titel II.4 Waar gaan uw gegevens naartoe);
- het bestaan van *geautomatiseerde besluitvorming*, nuttige informatie over de onderliggende logica hiervan en de verwachte gevolgen van die verwerking voor de betrokkene.

3) De betrokkene heeft het recht om een gratis kopie te krijgen van zijn of haar persoonsgegevens die de KMO verwerkt. Vraagt de betrokkene om extra kopieën, dan mag de KMO een redelijke vergoeding aanrekenen die niet hoger is dan de administratieve kost hiervan. Wanneer de betrokkene een verzoek elektronisch indient, deelt de KMO de informatie mee in een gangbaar elektronische formaat, tenzij de betrokkene vraagt om een kopie op een andere fysieke drager (bijvoorbeeld papier). Alvorens de kopie te versturen, moet de KMO nagaan of deze mededeling geen afbreuk doet aan de rechten en vrijheden van andere betrokkenen (bijv. indien er informatie over meer dan één persoon in eenzelfde bestand wordt verwerkt).

- **VOORBEELD:**
  - een personeelslid van de KMO vraagt toegang tot zijn of haar personeelsdossier en wil hiervan een gratis kopie krijgen. De KMO bezorgt een kopie van het personeelsdossier samen met een toelichting van de verwerking (zie punt 2) hierboven).

Voor meer info

- Artikel 13 AVG – Recht van inzage van de betrokkene

3 Het recht op verbetering

De betrokkene heeft het recht om onjuiste gegevens te verbeteren of onvolledige gegevens aan te vullen, onder meer door een aanvullende verklaring toe te voegen. Als de KMO deze persoonsgegevens heeft doorgegeven aan derde partijen, moet zij deze op de hoogte brengen van de aangebrachte verbetering, tenzij dit onmogelijk is of onevenredig veel inspanning vergt.

- **VOORBEELD**: een klant meldt aan een KMO dat hij/zij is verhuisd. De KMO moet het adres in haar klantenbestand aanpassen.

Voor meer info

- Artikel 16 AVG – Recht op rectificatie
- Artikel 19 AVG – Kennisgevingsplicht inzake rectificatie, wissing of verwerkingsbeperking

4 Het recht op gegevenswissing

Een betrokkene kan eisen dat de KMO persoonsgegevens wist waarvoor geen gegronde reden meer bestaat om deze te verwerken. Het recht om gegevens te wissen is niet absoluut. De betrokkene kan dit recht slechts in de onderstaande gevallen uitoefenen:

- de persoonsgegevens zijn niet langer noodzakelijk om het nagestreefde **doel** te vervullen;
- de KMO verwerkt de persoonsgegevens **onrechtmatig**;
- de KMO moet de persoonsgegevens wissen door toedoen van een **wettelijke verplichting**;
- de betrokkene **trekt de toestemming in** en de verwerking heeft geen andere rechtsgrond;
- na een succesvolle uitoefening van het recht van **bezwaar** (zie titel III.6 Recht van bezwaar);
- **minderjarigen** die toestemming gaven om een online dienst te gebruiken kunnen steeds vragen om die persoonsgegevens te wissen (ongeacht hun huidige leeftijd).

Gaf u de gewiste gegevens voordien door aan iemand anders? Dan moet de KMO deze ontvangers op de hoogte brengen van de gegevenswissing, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

- **VOORBEELD**: een betrokkene schrijft zich in op een sociaalnetwerksite. De betrokkene beslist om de sociaalnetwerksite te verlaten en vraagt het bedrijf om alle persoonsgegevens te verwijderen. Het bedrijf moet gevolg geven aan dit verzoek.

De KMO mag ook weigeren om de persoonsgegevens te wissen wanneer de verwerking noodzakelijk is voor onder andere:

- de uitoefening van het recht op vrijheid van meningsuiting en informatie;
- de instelling, uitoefening en de onderbouwing van een vordering in rechte;
- de vervulling van een wettelijke plicht of een taak van algemeen belang die op de KMO rust;
- onderzoek, statistiek, volksgezondheid, archivering in het algemeen belang – onder specifieke voorwaarden.

- **VOORBEELD**: een net ontslagen personeelslid vraagt om al zijn/haar persoonsgegevens te wissen uit het personeelsdossier. De KMO is echter wettelijk verplicht om een aantal sociale documenten (personeelsregister, individuele rekening, kopie van loonstaten enz.) gedurende vijf jaar te bewaren. Voor deze documenten moet de KMO het verzoek om gegevenswissing weigeren.

Voor meer info

- Artikel 17 AVG – Recht op gegevenswissing
- Artikel 19 AVG – Kennisgevingsplicht inzake rectificatie, wissing of verwerkingsbeperking

5 Het recht op beperking van gegevensverwerking

In bepaalde omstandigheden kan de betrokkene een "beperking" van de gegevensverwerking eisen. De beperking bevriest de gegevensverwerking. Bijgevolg mag de KMO de persoonsgegevens alleen nog maar opslaan en moet zij alle andere verwerkingsactiviteiten stopzetten.

De betrokkene heeft het recht om de beperking van de gegevensverwerking te verkrijgen wanneer:

- de betrokkene de **juistheid** van de persoonsgegevens betwist, gedurende een periode die de KMO in staat stelt de juistheid van de persoonsgegevens te controleren;
- de verwerking **onrechtmatig** is, kan de betrokkene in de plaats van de wissing van de gegevens, verzoeken om het gebruik van de persoonsgegevens te beperken;
- de KMO de persoonsgegevens niet meer nodig heeft, maar de betrokkene wel voor de uitoefening van **een rechtsvordering**;
- de betrokkene zijn recht van **bezwaar** uitoefent. De beperking geldt in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de KMO zwaarder wegen dan die van de betrokkene.

Indien de betrokkene het recht op beperking succesvol uitoefent, mag de KMO de gegevens enkel nog gebruiken met de toestemming van de betrokkene of voor de instelling van een rechtsvordering[5]. Gaf u de "bevroren" gegevens voordien door aan iemand anders? Dan moet de KMO deze ontvangers op de hoogte brengen van de verwerkingsbeperking, tenzij dit onmogelijk is of onevenredig veel inspanning vergt

Voor meer info

- ❖ Artikel 18 AVG – Recht op beperking van de verwerking
- ❖ Artikel 19 AVG – Kennisgevingsplicht inzake rectificatie, wissing of verwerkingsbeperking

6 Het recht van bezwaar

Iedere betrokkene kan bezwaar maken tegen de verwerking van persoonsgegevens die op hem of haar betrekking hebben "*vanwege met zijn specifieke situatie verband houdende redenen*". Het recht van bezwaar kan uitsluitend uitgeoefend worden wanneer de verwerking steunt op één van de volgende rechtsgronden:

- het gerechtvaardigde belang van de KMO of een derde;
- de vervulling van een taak van algemeen belang of het openbaar gezag.

In andere gevallen kan de betrokkene geen bezwaar maken omdat voor de overige rechtsgronden alternatieven bestaan om hetzelfde doel bereiken: bij toestemming kan de betrokkene deze intrekken; tegen verwerking die de wet oplegt kan de betrokkene geen bezwaar maken.

De uitoefening van het recht op bezwaar dwingt de KMO tot een belangenafweging. De KMO staakt iedere verwerking van de persoonsgegevens tenzij zij dwingende gronden kan opwerpen die zwaarder wegen dan de rechten en vrijheden van de betrokkene (bijv. een vordering in rechte). De KMO moet deze gronden documenteren en meedelen aan betrokkene.

⚠ Op deze belangenafweging bestaat een belangrijke uitzondering in het voordeel van de betrokkene: bij **direct marketing** heeft de betrokkene altijd het recht om zonder enige motivering bezwaar aan te tekenen. Dit bezwaar leidt dan automatisch tot de stopzetting van de verwerking voor dit doeleinde.

⚠ De KMO moet de mogelijkheid tot het uitoefenen van het recht op bezwaar, duidelijk en apart van ander informatie onder de aandacht van de betrokkene brengen. Bijv. door in het oog springende knop

5 De gegevens mogen ook nog verwerkt ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of een lidstaat (artikel 18(2) AVG).

- **VOORBEELD:**

  - De betrokkene koopt online een ticket voor een optreden van een band. Nadien ontvangt de betrokkene advertenties voor concerten en evenementen. De betrokkene wenst die reclame niet meer te ontvangen en tekent bezwaar aan. De KMO moet de direct marketing beëindigen.

  - In de verzekeringssector zijn persoonsgegevens in bepaalde situaties nodig voor de bestrijding van witwaspraktijken. Een verzekeringsmakelaar kan daarom soms weigeren om gevolg te geven aan een bezwaar omdat antiwitwaswetgeving hem verplicht de gegevens bij te houden.

Voor meer info

- Artikel 21 AVG – Recht van bezwaar

7 Het recht op gegevensoverdraagbaarheid

Het recht op gegevensoverdraagbaarheid stelt de betrokkene in staat om zijn/haar persoonsgegevens te verkrijgen en te hergebruiken voor andere diensten. Op een gebruiksvriendelijke manier kan de betrokkene persoonsgegevens verplaatsen van de ene IT-omgeving naar een andere.

Het recht op gegevensoverdraagbaarheid kan alleen worden uitgeoefend indien aan drie voorwaarden gelijktijdig is voldaan:

- ✓ de verwerking vindt plaats op basis van de toestemming of een overeenkomst;
- ✓ het gaat om een geautomatiseerde verwerking (geen papieren documenten); *en*
- ✓ de betrokkene verstrekt de gegevens zelf. Dit betekent dat dit recht alleen slaat op de persoonsgegevens:
  - die de betrokkene zelf bewust heeft verstrekt (bijv. bij registratie: naam, adres, etc....);
  - die de KMO observeert op basis van het gedrag van de betrokkene (bijv. wearable);
  - dit recht slaat niet op data die de KMO zelf ontwikkelt op basis van bovenstaande data.

De betrokkene krijgt het recht om zijn persoonsgegevens:

- te verkrijgen in een gestructureerde, gangbare en machinaal leesbare vorm. De vorm moet de betrokkene in staat stellen om de persoonsgegevens te hergebruiken voor een andere dienst;
  - **VOORBEELD**: XML, JSON en CSV zijn courante formats die voldoen aan dit criterium. Ook metadata moet worden doorgestuurd zodat de data kan functioneren op een ander platform. Een Pdf-formaat volstaat niet.
- rechtstreeks te laten overdragen aan een andere verwerkingsverantwoordelijke. De KMO moet dit alleen doen in zoverre een dergelijke rechtstreekse overdracht technisch mogelijk is.

- **VOORBEELD**:
  - een consument kan de overdracht vragen van zijn songlist van een online muziek streaming dienst.
  - een KMO die een webmail dienst aanbiedt moet de adressenlijst en de e-mails van de betrokkene overdragen aan een andere webmail dienst op voorwaarde dat dit technisch mogelijk is. Zo niet, bezorgt de KMO de adressenlijst aan de betrokkene in een courant, herbruikbaar digitaal formaat.

Voor meer info

- Artikel 20 AVG – Recht op overdraagbaarheid van gegevens
- Richtlijnen van de WP29 over het recht op gegevensoverdraagbaarheid – WP242

8 Het recht om niet aan geautomatiseerde besluitvorming onderworpen te worden

Een betrokkene mag niet onderworpen worden aan een volledig automatische beslissing – zonder menselijke tussenkomst – die hem of haar aanzienlijk treft of juridische gevolgen heeft.

Profilering kan soms gepaard gaan met geautomatiseerde besluitvorming. Profilering verwijst naar: *"elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen"* (artikel 4(4) AVG).

Om zich te beroepen op dit verbod moet het gaan om:

- een beslissing die uitsluitend op een geautomatiseerde verwerking berust, zonder menselijke tussenkomst. Dit betekent dat een fysieke persoon geen betekenisvolle controle uitoefent op de beslissing en bijvoorbeeld de beslissing niet kan wijzigen of annuleren.
- een beslissing die voor de betrokkene rechtsgevolgen teweeg brengt of die hem op een andere manier aanzienlijk treft.
    - **VOORBEELD**: *rechtsgevolgen*: de automatisch ontbinding van een telefonie-contract omdat de klant de maandelijkse factuur niet betaalde.
    - **VOORBEELD**: *aanzienlijk treffen*: In de onderstaande gevallen *kan* de beslissing de betrokkene aanzienlijk treffen, maar dit hangt steeds af van de context:
        - de automatische weigering van een betalingskrediet bij een online aankoop;
        - de automatische weigering van sollicitanten die solliciteren via een online platform;
        - prijsdifferentiatie op basis van het surf- en aankoopgedrag van een consument.

In drie situaties is het toch toegestaan om geautomatiseerde individuele besluitvorming toe te passen:

- als een wet dit toelaat (bijvoorbeeld voorkoming van belastingfraude en-ontduiking);
- als de besluitvorming berust op een uitdrukkelijke toestemming van de betrokkene; of
- als dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst.
    - Let op: deze laatste situatie hangt steeds af van een afweging *in concreto*. Van zodra minder privacy-intrusieve methoden bestaan om de overeenkomst te sluiten of uit te voeren, is de maatregel niet langer 'noodzakelijk'.

Past een KMO in één van deze drie gevallen geautomatiseerde besluitvorming toe, dan moet deze voorzien in passende maatregelen die de rechten van de betrokkene beschermen. Die maatregelen omvatten minstens de mogelijkheid voor de betrokkene om dit besluit aan te vechten, zijn of haar standpunt kenbaar te maken en een menselijke tussenkomst te vragen.

⚠ Bij gevoelige gegevens is geautomatiseerde besluitvorming alleen mogelijk op basis van uitdrukkelijk toestemming of een zwaarwegend algemeen belang op grond van Unierecht of nationaal recht.

Voor meer info

- ❖ Artikel 22 AVG – Geautomatiseerde besluitvorming, waaronder profilering
- ❖ Richtlijnen van de WP29 over geautomatiseerde besluitvorming

IV. Wat als het fout loopt?

1 Een data breach – documenteer en meld het!

Iedere KMO moet procedures invoeren om bepaalde inbreuken in verband met persoonsgegevens (ook wel data breach genoemd) te melden. De AVG omschrijft een data breach als een inbreuk op de beveiliging die per ongeluk of met opzet leidt tot een vernietiging, verlies, wijziging of ongeoorloofde toegang of doorgifte van persoonsgegevens. Een inbreuk komt gemakkelijker voor dan je denkt:

- **VOORBEELD**: Voorbeelden van een data breach zijn:
  - een cyberaanval waarbij ransomware de toegang tot de IT-infrastructuur blokkeert;
  - een verloren of gestolen bedrijfslaptop, USB-stick of CD met persoonsgegevens;
  - een ernstige stroomuitval heeft tot gevolg dat de toegang tot de servers wegvalt;

De KMO moet elke data breach – ook de allerkleinste – bijhouden in een **intern logboek**. Dit logboek vermeldt: de oorzaak, de getroffen persoonsgegevens, de gevolgen en de genomen maatregelen. Daarnaast valt het aan te raden om de reden om een data breach al dan niet te melden hier ook op te nemen. Dit logboek kan geïntegreerd worden in het register van verwerkingsactiviteiten.

Bovendien moet de KMO in bepaalde situaties de inbreuk ook **melden**:

- **aan de GBA**: als de data breach waarschijnlijk **een risico** inhoudt voor de rechten en vrijheden van de betrokkene;
- **aan de betrokkene**: als de data breach waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van de betrokkene.

1.1 Melden aan de GBA

Een KMO moet een data breach melden aan de GBA als de inbreuk waarschijnlijk **een risico** inhoudt voor de rechten en vrijheden van de betrokkene.

Is de KMO verwerkingsverantwoordelijke, dan moet de melding gebeuren binnen de 72 uur nadat de KMO op de hoogte is van de data breach. Zo mag een KMO een melding van een klant m.b.t. een mogelijke data breach eerst verifiëren voordat zij officieel op de hoogte is en de termijn van 72 uur loopt. Is de KMO een verwerker dan meldt deze de data breach meteen aan de verwerkings-verantwoordelijke.

De melding vermeldt minstens: tijdstip van de data breach, tijdstip waarop de KMO op de hoogte was, de vermoedelijke oorzaak, de getroffen persoonsgegevens, de gevolgen, de genomen maatregelen en de contactgegevens van de persoon die de data breach opvolgt binnen de KMO. De KMO die op de hoogte is van een data breach, maar nog niet over al deze informatie beschikt, mag al overgaan tot melding en de overige informatie later bezorgen.

- **VOORBEELD:**
  - bij een inbraak wordt een geëncrypteerde CD gestolen met personeelsgegevens. De KMO heeft een back-up van de gegevens. Zolang de encryptiesleutel niet wordt gestolen of gekraakt is een melding bij gebrek aan risico niet noodzakelijk;
  - een KMO met een online webshop krijgt een melding van een klant die een verdachte mail ontving om een factuur te betalen. De KMO stelt na kort onderzoek vast dat een derde haar klantengegevens systematisch onderschept. Nu is de KMO op te hoogte van de data breach en meldt dit binnen 72 uur aan de GBA en haar getroffen klanten.

1.2 Melden aan de betrokkene

Een KMO moet een data breach melden aan de getroffen individuen als de data breach waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van de betrokkene. Dit is echter niet noodzakelijk als:

- de KMO veiligheidsmaatregelen had voorzien om toe te passen bij een data breach, zoals bijvoorbeeld een sterke encryptiemethode;

- de KMO na de data breach maatregelen nam waardoor het hoge risico zich waarschijnlijk niet meer zal voordoen (bijv. wissen op afstand bij diefstal van drager);
- de individuele mededeling zou onevenredige inspanningen vergen. Een openbare mededeling is in dit geval aangewezen om de betrokkenen te informeren.

o **VOORBEELD:**

  – een KMO verzamelt door middel van wearables gegevens over slaap, eetgewoonten en fysieke activiteit en leidt hieruit gezondheidsinformatie af. De transmissie van deze gegevens blijkt onveilig en hackers hebben de ruwe data, samen met de gebruikersprofielen online gepubliceerd. In dit geval is het risico voldoende hoog om niet alleen de GBA maar ook de gebruikers op de hoogte te brengen.
  – een hacker verkrijgt toegang tot de personeelsgegevens van een marketingbedrijf. De intrusie wordt gedetecteerd. Het gaat om: adres, gezinssamenstelling, salaris en ziekteverloven. Het bedrijf licht de GBA in binnen de 72 uur en brengt ook het personeel op de hoogte.

1.3 Wanneer is er een (hoog) risico?

De volgende criteria zijn relevant om te bepalen of er sprake is van een waarschijnlijk (hoog) risico in geval van een data breach. Deze lijst is niet exhaustief en in de praktijk zal de KMO altijd een feitelijke afweging moeten maken in functie van het concrete geval. Daarom net is het van belang om de reden van niet-melden ook op te nemen in het logboek van de inbreuken in verband met persoonsgegevens.

- de gevoeligheid van de gelekte data: bv. gegevens m.b.t. financiële situatie, gezondheid, identiteitsdocumenten;
- de hoeveelheid van de gelekte data: bepaalde gegevens kunnen afzonderlijk onschuldig zijn, maar in combinatie niet;
- de mogelijke gevolgen voor een individu: identiteitsdiefstal, fraude, reputatieschade of vernedering;
- het aantal getroffen individuen;
- de kwetsbaarheid van individuen: persoonsgegevens van kinderen, ouderlingen of gehandicapte personen;
- het gemak om individuen te identificeren: zijn de gegevens al dan niet versleuteld of gecodeerd?

Voor meer info

❖ Artikel 33-34 AVG – Melding van een inbreuk in verband met persoonsgegevens
❖ Richtlijnen van de WP29 over de melding van een inbreuk in verband met persoonsgegevens onder Verordening 2016/679 – WP250

2 Een overtreding van de AVG

Bij een overtreding van de AVG kan de betrokkene beroep doen op twee parallelle afdwingings-mechanismen. De betrokkene die meent dat de verwerking van zijn/haar persoonsgegevens inbreuk maakt op de AVG kan een klacht tot de GBA richten die kan uitmonden in een sanctie voor de KMO of schadevergoeding eisen via de gewone rechtbank. Niets sluit uit dat betrokkenen tegelijkertijd een klacht indienen bij de GBA en zich richten tot de rechter.

2.1 Sancties

De GBA kan verschillende sancties opleggen bij een niet-naleving van de AVG. Naar aanleiding van een klacht of op eigen initiatief kan de GBA onder andere:

- een waarschuwing of berisping geven;
- dwingen om een verzoek van de betrokkene in te willigen;
- dwingen om binnen een bepaalde termijn de verwerking AVG-conform te maken;
- de verwerking bevriezen of verbieden;
- boetes opleggen tot 2% of 4% van de jaaromzet, afhankelijk van de inbreuk.

De KMO heeft een plicht om medewerking te verlenen bij een eventueel onderzoek van de GBA (artikel 31 AVG). Indien u het niet eens bent met een juridisch bindende beslissing van de GBA die aan u gericht is, kan u een voorziening in rechte instellen tegen die beslissing (artikel 78 AVG).

2.2 Schadevergoeding

Iedere persoon die schade lijdt door een inbreuk op de AVG, kan een schadevergoeding eisen voor de rechtbank (artikel 79 AVG).

Indien er meerdere verwerkingsverantwoordelijke en/of verwerkers betrokken zijn bij eenzelfde verwerking kan betrokkene zich zowel tot de verwerkingsverantwoordelijke als de verwerker richten (artikel 82 AVG). Elke betrokken verwerkingsverantwoordelijke of verwerker is aansprakelijk voor de gehele schade ten opzichte van het getroffen individu, tenzij zij kunnen bewijzen op geen enkele manier verantwoordelijk te zijn voor de geleden schade.

Na de volledige vergoeding van het getroffen individu, kunnen de verwerkingsverantwoordelijke en de verwerker onderling verhaal uitoefenen. De verwerkingsverantwoordelijke of verwerker die de schade geheel heeft vergoed, kan het deel van de schadevergoeding dat overeenkomt met hun deel van de aansprakelijkheid voor de schade verhalen op andere verwerkingsverantwoordelijken of verwerkers die bij de verwerking waren betrokken.

Let dus op: ook als het probleem zich situeert op het niveau van uw verwerker – de betrokkene kan zich tot de KMO die verwerkingsverantwoordelijke is, wenden!

- **VOORBEELD**: een in België gevestigde KMO slaat gevoelige klantengegevens op bij een datacenter. Er doet zich bij het datacenter een data breach voor, waarbij de klantengegevens van de KMO worden getroffen. De klant kan zich richten tot de Belgische KMO om schadevergoeding te bekomen. Nadien kan de KMO zich keren tegen het datacenter om een deel van de betaalde schadevergoeding terug te vorderen.

Voor meer info

- Hoofdstuk VIII AVG – Beroep, aansprakelijkheid en sancties
- Richtlijnen van de WP29 over de berekening en oplegging van administratieve boetes onder Verordening 2016/679 – WP253

V. Checklist voor de verwerker

De voornaamste verplichtingen die voor de verwerker gelden zijn:

- ✓ Sluit een **waterdicht contract** af met de verwerkingsverantwoordelijke. Dit is een verplichting. Zie titel II.3.1 Sluit een contract af voor een minimale inhoud van dit contract. Als verwerker mag u de persoonsgegevens niet gebruiken voor doeleinden die niet zijn opgenomen in dit contract. Doet u dit toch, dan wordt u zelf als verwerkingsverantwoordelijke beschouwd voor die nieuwe doeleinden.
- ✓ Werk je zelf met **onderaannemers** of verwerkers? Dat kan natuurlijk, maar hou rekening dat de verwerkingsverantwoordelijke hier vooraf mee akkoord moet gaan.
- ✓ **Veiligheid** is een uiterst belangrijke verplichting voor een verwerker. Ook de verwerker moet passende technische en organisatorische maatregelen nemen om een veilige verwerking van de persoonsgegevens te waarborgen. Zie titel II.1.7 Beveiliging voor voorbeelden van gepaste veiligheidsmaatregelen.
- ✓ Bewaar of verplaats je persoonsgegevens **buiten de Europese Unie**? Meld dit aan de verwerkingsverantwoordelijke en ga na of u zich kan beroepen op één van de mechanismen voor de doorgifte van persoonsgegevens buiten de Europese Unie (zie titel II.4 Waar gaan uw gegevens naartoe?).
- ✓ De verplichting om een **register van de verwerkingsactiviteiten** bij te houden geldt op dezelfde manier voor verwerkers als voor verwerkingsverantwoordelijken (zie titel II.2.1 stap 1: Maak een overzicht met het register van verwerkingsactiviteiten).
- ✓ Verwerkers moeten zelf nagaan of zij al dan niet **een DPO** moeten aanstellen. Het feit dat de verwerkingsverantwoordelijke geen DPO aanstelt betekent niet dat de verwerker evenmin een DPO moet aanstellen (zie titel II.2.2 stap 2: Duid een functionaris voor de gegevens-bescherming (DPO) aan).
- ✓ De verplichting tot het uitvoeren van **een GEB** rust in de eerste plaats op de verwerkings-verantwoordelijke. De verwerker moet de verwerkingsverantwoordelijke wel bijstaan in de uitvoering van de GEB.

- ✓ De verplichtingen in verband met het houden van een logboek en het melden van **inbreuken in verband met persoonsgegevens** zijn in de eerste plaats gericht tot de verwerkings-verantwoordelijken. De verwerker moet de verwerkingsverantwoordelijke bijstaan in de naleving van die verplichtingen en moet de inbreuk zonder onredelijke vertraging melden aan de verwerkingsverantwoordelijke (zie titel IV.1 Een data breach).

- ✓ Naast het opleggen van verplichtingen, kent de AVG **rechten** toe aan elke betrokkene (zie titel III Rechten van de betrokkene). De betrokkene richt zich voor de uitoefening van die rechten tot de verwerkingsverantwoordelijke. De verwerker moet de verwerkingsverantwoordelijke echter bijstaan om de uitoefening van die rechten mogelijk te maken.

- ✓ Op de verwerker rust ook een **medewerkingsplicht** ten opzichte van de GBA.

- ✓ Tot slot moet de verwerker **de verwerkingsverantwoordelijke ook bijstaan** voor de naleving van een aantal verplichtingen door deze laatste:

    - de beveiliging van de verwerking door de verwerkingsverantwoordelijke;
    - de uitoefening van de rechten door betrokkenen (zie hierboven);
    - de logging en de meldingsplicht voor inbreuken (zie hierboven) ;
    - het uitvoeren van een GEB door de verwerkingsverantwoordelijke;
    - het verstrekken van informatie aan de GBA bij een voorafgaande raadpleging in het kader van de GEB.