Els Kindt - Pauline Hellemans

CiTiP, KU Leuven

26 Juli 2020

FAQ-BROCHURE VOOR KMO'S

Project BOOST – Boost het bewustzijn van de Belgische KMO's en de naleving van de AVG, met speciale aandacht voor drie nalevingsthema's

Autorité de protection des données
Gegevensbeschermingsautoriteit

UNIVERSITÉ DE NAMUR

VUB VRIJE UNIVERSITEIT BRUSSEL

KU LEUVEN

Dit project wordt gefinancierd door het programma Rechten, gelijkheid en burgerschap REC-AG-2019 van de Europese Unie.

FAQ-BROCHURE VOOR KMO'S

Els Kindt
CiTiP, KU Leuven

Pauline Hellemans
CiTiP, KU Leuven

26 Juli 2020

1. INLEIDING

Deze publicatie werd ontwikkeld in het kader van het BOOST-project (januari – december 2020) en geeft meer uitleg over de toepassing en over bepaalde verplichtingen van de Algemene Verordening Gegevensbescherming (AVG). Ze is bestemd voor kleine en middelgrote ondernemingen (KMO's) in België en is een aanvulling op de eerdere publicatie Wegwijs in de AVG voor KMO's van de Gegevensbeschermingsautoriteit (GBA). Ze verduidelijkt bepaalde aspecten en verplichtingen onder de AVG, met bijkomende voorbeelden en verwijzing naar recente bijkomende richtlijnen en beslissingen.

Deze brochure behandelt de AVG niet volledig, maar zoomt enkel in op een aantal belangrijke onderwerpen. Deze werden gekozen op basis van de BOOST-projectomschrijving en een bevraging in BOOST van de AVG-kennis en de huidige knelpunten bij KMO's. Er wordt aandacht besteed aan:

- de begrippen 'verwerkingsverantwoordelijke' en 'verwerker',
- het transparantiebeginsel,
- de gegevensbeschermingseffectbeoordeling,
- het verwerkingsregister, en
- de Data Protection Officer (DPO).

Deze onderwerpen worden verduidelijkt in de vorm van vragen en antwoorden.

Dit project werd gesponsord door het EU-programma Rechten, Gelijkheid en Burgerschap REC-AG-2019, onder grant agreement nummer 874505.

WAT IS DE ALGEMENE VERORDENING GEGEVENSBESCHERMING?

De Algemene Verordening Gegevensbescherming (hierna **AVG**), soms ook gekend als de **GDPR**, is wetgeving van de Europese Unie. U kan hier de volledige AVG vinden.

De AVG legt verplichtingen op om 'persoonsgegevens' **te beschermen** en de **fundamentele rechten** van personen in de EU **respecteren,** waarbij het vrij verkeer van persoonsgegevens eveneens wordt nagestreefd.

De AVG is van **toepassing sinds 25 mei 2018** en werd in België verder aangevuld met o.a. de wet van 30 juli 2018 (hierna **Gegevensbeschermingswet 2018**). U kan hier de Gegevensbeschermingswet 2018 raadplegen.

2. MOET MIJN ONDERNEMING DE AVG NALEVEN?

Elke onderneming, organisatie, vereniging of persoon die 'persoonsgegevens' geautomatiseerd of in bestanden 'verwerkt' moet de AVG naleven. Aangezien het toepassingsgebied van de AVG ruim is, zal in de praktijk zo goed als elke onderneming de AVG moeten naleven. Hier vindt U een video waarin dit toepassingsgebied verder wordt toegelicht.

Wettelijke basis: artikel 2, 1. AVG

De AVG is niet enkel van toepassing op ondernemingen, maar ook op organisaties en verenigingen (zoals VZW's). Wanneer in deze FAQ-brochure het begrip 'onderneming' wordt gebruikt, wordt hier telkens ook vereniging en organisatie mee bedoeld.

Voorbeeld 1: zodra een onderneming één van de volgende activiteiten uitvoert, voor eigen rekening of in opdracht van een derde, dient de onderneming, als verantwoordelijke of verwerker, de AVG na te leven:

- Het opslaan en verwerken 'op de computer' van gegevens van klanten (bijv. klantenlijsten en facturatiegegevens met namen van personen en bijhorende e-mailadressen, ...) en/of van leveranciers (bijv. leverancierslijsten met namen van personen) of het bijhouden van deze gegevens op geordende papieren fiches;

- Het ontvangen, online of offline, opslaan en gebruiken op de computer van werknemersgegevens, zoals loonfiches of curriculum vitae gegevens van 'kandidaatwerknemer'; het online opvragen en opslaan van HR-gegevens van werknemers bij een payrollbedrijf;

- Het houden van een website op een eigen server of op platformen van derden (bijv. een Facebookpagina) met vermelding of inzameling (bijv. via cookies) van persoonsgegevens.

Voorbeeld 2: Een VZW die bijvoorbeeld de volgende activiteiten uitoefent dient de AVG na te leven:

- De contactgegevens van haar leden verzamelt om vergaderingen te organiseren;
- De gegevens van leveranciers bijhoudt om leveringen af te handelen;
- Gegevens betreffende de vergoedingen van vrijwilligers bijhoudt en gebruikt om deze vergoedingen uit te betalen;
- Gegevens bijhoudt van de bezoekers van de activiteiten georganiseerd door de VZW of van de lokalen van de VZW.

De AVG is dus van toepassing op alle ondernemingen, inclusief KMO's, die persoonsgegevens verwerken. De **grootte of het soort activiteiten van de onderneming is hierbij in principe niet belangrijk**. Weliswaar zijn er voor kleine en middelgrote ondernemingen enkele vereisten soepeler, in het bijzonder vooral wat de aanstelling betreft van een gegevensbeschermingsfunctionaris.

WAT ZIJN 'PERSOONSGEGEVENS'?

Persoonsgegevens zijn alle gegevens en informatie over een **geïdentificeerde of identificeerbare persoon**. Dit is een **ruim** begrip. Iemand is identificeerbaar indien de informatie met 'redelijke inspanningen' kan gekoppeld worden aan en leiden tot de identificatie van de persoon, direct (bijv. via naam) of indirect (bijv. aan de hand van een klantennummer). Voor deze 'redelijkheidstoets' zijn zowel objectieve (vereiste tijd en technische middelen) als contextuele elementen (die dus van geval tot geval kunnen verschillen) van belang.

Wettelijke basis: Artikel 4, (1) AVG

Voorbeeld van persoonsgegevens: familienaam, e-mailadres, adres, rijksregisternummer, voorkeuren, IP-adres, surf en clickgedrag op een website, localisatiegegevens zoals bijvoorbeeld verkregen van een smartphone via een mobiele app, foto van een gezicht (bijv. een foto van een uitzendkracht), camerabeelden, ziektebriefje, personeelsevaluatie, uittreksel strafregister, loonfiche werknemer, ...

De technologische vooruitgang heeft ervoor gezorgd dat veel gegevens die **anoniem lijken dit niet zijn en toch persoonsgegevens zijn**, omdat ze natuurlijke personen toch kunnen identificeren, bijvoorbeeld door combinatie met andere persoonsgegevens of omwille van hun aard. Meer informatie vindt U ook hier.

Voorbeeld: Locatiegegevens van een smartphone zijn persoonsgegevens zelfs al lijken ze anoniem.

Voor meer richtlijnen omtrent de interpretatie van het gebruik van locatiegegevens voor tracing applicaties zie Advies 4/2020 van de EDPB op pagina 7.

WAT BETEKENT 'VERWERKEN'?

Verwerken van persoonsgegevens betekent **elke bewerking (of een geheel van bewerkingen) van (een set van) persoonsgegevens** (al dan niet uitgevoerd met behulp van geautomatiseerde systemen). Dit is een **ruim** begrip.

Wettelijke basis: Artikel 4, (2) AVG

Voorbeelden van verwerkingen: verzamelen, oplijsten, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door doorzenden, verspreiden of anderzijds beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van persoonsgegevens.

3. BEN IK 'VERWERKINGSVERANTWOORDELIJKE' OF 'VERWERKER' VOLGENS DE AVG?

De AVG onderscheidt twee belangrijke rollen: die van verwerkingsverantwoordelijke en van verwerker. Dit onderscheid is cruciaal, omdat de verwerkingsverantwoordelijke meer verantwoordelijkheid draagt en meer verplichtingen moet nakomen dan de verwerker.

WAT IS EEN (GEZAMENLIJKE) VERWERKINGSVERANTWOORDELIJKE?

De verwerkingsverantwoordelijke is de onderneming of entiteit die **beslist waarom of waarvoor** persoonsgegevens verzameld en gebruikt worden en **hoe** deze persoonsgegevens verwerkt worden. De verantwoordelijke neemt m.a.w. de beslissing over de **doeleinden en de middelen**.

Wanneer twee ondernemingen gezamenlijk over de middelen en doeleinden beslissen, dan zijn ze **gezamenlijke verantwoordelijken**. Wanneer ze elk afzonderlijk deze beslissingen nemen, zijn ze elk afzonderlijk verantwoordelijke. Gezamenlijke verantwoordelijken moeten onderling vastleggen wie de verplichtingen naar betrokken personen zal vervullen en dit ook kenbaar maken aan de betrokkenen.

Wettelijke basis: Artikelen 4, (7) en 26 AVG

Voor meer richtlijnen omtrent de interpretatie van de begrippen 'verwerker' en 'verantwoordelijke' zie Advies 1/2010 van de Werkgroep 29 en de richtlijnen 07/2020 van de EDPB.

Voorbeeld 1: Uw KMO beslist dat registratie voor toegang tot Uw website nodig is en verzoekt om naam en e-mailadressen via een online registratieprocedure *(hoe).* Deze gegevens zal U gebruiken om zelf reclame-e-mails te verzenden *(waarom/waarvoor).* Uw KMO is **verantwoordelijke**.

Voorbeeld 2: Een bakkerij beslist om voor haar klantenkaart samen te werken met een onderneming die een loyaliteitssysteem gratis aanbiedt en daarvoor persoonsgegevens verzamelt van het cliënteel van de bakkerij. De bakker treedt op als de verantwoordelijke voor de verwerkingen die de onderneming uitvoert voor het beheer van de gratis klantenkaart in opdracht van de bakker, en de onderneming als verwerker. Echter, in de mate dat de onderneming uw klantengegevens zelf hergebruikt voor eigen doeleinden, bijvoorbeeld om haar loyaliteitssysteem te verbeteren, is zij zelf **ook een verwerkingsverantwoordelijke** en zijn de bakkerij en de loyaliteitsfirma **elk afzonderlijk verwerkingsverantwoordelijken.**

Voorbeeld 3: Een marketingbedrijf verzamelt e-mailadressen en klikgegevens van websitebezoekers in opdracht en volgens de instructies van een KMO voor marketingdoeleinden. Het marketingbedrijf hergebruikt deze verzamelde gegevens en profielen evenwel om deze te combineren met andere klikgegevens van andere websites om door te verkopen aan andere klanten. Het marketingbedrijf en de KMO zijn dan **elk afzonderlijke verwerkingsverantwoordelijken.**

Voorbeeld 4: Een zelfstandig verzekeringen- en zakenkantoor beslist een facturatieapplicatie aangeboden door een platform te gebruiken. Het kantoor beslist samen met de platformaanbieder de persoonsgegevens te gebruiken voor reclamedoeleinden. Zowel het kantoor als de aanbieder van het platform treden op als **gezamenlijke verantwoordelijken**

voor het gebruik van de persoonsgegevens voor reclamedoeleinden.

Voorbeeld 5: Een zelfstandig verzekeringen- en zakenkantoor beslist een facturatie-applicatie aangeboden door een platform te gebruiken. De factuurapplicatie stelt facturen op voor het kantoor in opdracht van het kantoor. Het kantoor treedt op als **verantwoordelijke** en de applicatieaanbieder treedt op als **verwerker**.

WAT IS EEN 'VERWERKER'?

De verwerker is een onderneming of andere entiteit die persoonsgegevens **enkel en alleen ten behoeve van** en **in opdracht van** een **andere onderneming** verwerkt. Merk op dat een verwerkingsverantwoordelijke die een verwerker aanstelt een verwerkingsovereenkomst dient te ondertekenen met deze verwerker.

Wettelijke basis: Artikel 4, (8) en 28 AVG

Voorbeeld 1: Het marketingbedrijf Y verzamelt e-mailadressen via websites van derden speciaal in opdracht van onderneming X voor de uitsluitende doeleinden en volgens de instructies van onderneming X. Het marketingbedrijf Y treedt op als verwerker voor deze inzameling.

Voorbeeld 2: Een payrollbedrijf verwerkt persoonsgegevens voor een KMO. Het payrollbedrijf zal optreden als een verwerker indien het de persoonsgegevens enkel en alleen in opdracht van de KMO verwerkt. De KMO bepaalt de doeleinden en middelen van de gegevensverwerking, en is daarmee verwerkingsverantwoordelijke.

Voorbeeld 3: Een websiteontwikkelaar ontwikkelt websites in opdracht van ondernemingen. Bij het opstellen en onderhouden van deze websites registreert de websiteontwikkelaar in opdracht van die onderneming bezoekersgegevens. Indien de websiteontwikkelaar de bezoekersgegevens uitsluitend voor de ondernemingen verwerkt, zal de websiteontwikkelaar als verwerker optreden. De ondernemingen treden dan op als verwerkingsverantwoordelijke.

Voorbeeld 4: Een onderneming bewaart haar klantgegevens niet op lokale servers maar in de *cloud* bij een hosting provider. Deze hosting provider zal optreden als een verwerker indien deze de gegevens niet voor eigen doeleinden gebruikt.

Voor meer richtlijnen omtrent de interpretatie van de begrippen 'verwerker' en 'verantwoordelijke' zie de Advies 1/2010 van de Werkgroep 29 en de richtlijnen 07/2020 van de EDPB.

ARREST *FASHION ID* VAN HET EHVJ

Het Europese Hof van Justitie (EHvJ) heeft in 'Fashion ID' het begrip 'gezamenlijke verwerkingsverantwoordelijken' (Artikel 26 van de AVG) verduidelijkt. Het EHvJ heeft met name bepaald dat een onlineverkoopbedrijf dat Facebook's 'Like'-button (ook wel 'third party plugin' genoemd) op zijn website heeft geïntegreerd, samen met Facebook aansprakelijk is voor de verwerking van de persoonsgegevens van de gebruikers van de website. Deze gezamenlijke aansprakelijkheid is in dit geval weliswaar beperkt tot het verzamelen van gegevens via de website en de overdracht ervan naar Facebook.

Hieruit volgt dat elke KMO die dergelijke 'plug-ins' op haar website invoert, gezamenlijke verantwoordelijk is, met Facebook, en verplicht is om, om in afspraak met Facebook:

- aan de gebruikers de vereiste informatie mee te delen over de verwerkingen van hun gegevens, ook de verwerkingen door Facebook, en
- wanneer dit vereist is, een geldige toestemming te verkrijgen van de gebruikers vooraleer de gegevens worden ingezameld en doorgegeven.

U kan het arrest van het EHvJ hier volledig lezen.

4. WELKE VERPLICHTINGEN MOET MIJN ONDERNEMING NALEVEN ONDER DE AVG?

De AVG legt verschillende verplichtingen op aan alle ondernemingen die persoonsgegevens verwerken, zowel als ze verantwoordelijke zijn als verwerker. Het naleven van de AVG gaat dus verder dan alleen het opstellen van een privacyverklaring. Over deze verklaring, hieronder meer.

Het naleven van de AVG vraagt dus globaal genomen een **grondige proactieve en steeds terugkerende analyse** van alle persoonsgegevensstromen en -processen binnen een onderneming en vervolgens acties voor de naleving van alle wettelijke verplichtingen op basis van deze analyses en evaluaties onder het gegevensbeschermingsrecht. Bovendien moet een verwerkingsverantwoordelijke steeds kunnen **bewijzen en aantonen** dat de onderstaande verplichtingen worden nageleefd in zijn onderneming.

Hieronder herhalen we de voornaamste verplichtingen **kort** en in het algemeen:

I. De zeven algemene beginselen ('geboden') van artikel 5 AVG

- Persoonsgegevens verwerken op een **rechtmatige, behoorlijke en transparante** wijze;

WAT IS EEN RECHTMATIGE VERWERKING EN WAT ZIJN VERWERKINGSGRONDEN?

Opdat persoonsgegevens rechtmatig verwerkt worden, moet **aan minstens één** van de volgende **verwerkingsgronden** van de AVG voldaan zijn (artikel 6 AVG) **(en voor gevoelige persoonsgegevens is eveneens een uitzonderingsgrond vereist onder artikel 9 AVG)**:

- De betrokkene verleende **toestemming** voor de verwerking (zie ook hier op p. 8);
- De verwerking is *noodzakelijk* voor de **uitvoering van een overeenkomst** met betrokkene, of maatregelen daaraan voorafgaand (zie ook hier op p. 9);
- De verwerking is *noodzakelijk* voor een **wettelijke verplichting** die rust op de verwerkingsverantwoordelijke (zie ook hier op p. 9);
- De verwerking is *noodzakelijk* zijn om de **vitale belangen** van een betrokkene of van een natuurlijk persoon te beschermen;
- De verwerking is *noodzakelijk* voor een **taak** van **algemeen belang** (zoals bijv. volksgezondheid, sociale bescherming en het beheer van gezondheidszorgdiensten) of **taak voor uitoefening van openbaar gezag** van de verantwoordelijke;
- De verwerking is *noodzakelijk* voor een **gerechtvaardigd belang** van de verwerkingsverantwoordelijke of derde, en de belangen of grondrechten van betrokkene wegen niet door, in het bijzonder wanneer dit een kind is (zie ook hier op p. 10).

- Persoonsgegevens slechts verzamelen voor **welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden** en deze verder enkel verwerken voor doeleinden die **verenigbaar** zijn met de oorspronkelijke doeleinden **(doelbinding)** (zie ook hier op p. 10);
- Enkel persoonsgegevens die **toereikend, relevant en noodzakelijk** voor de doeleinden verwerken (**minimale gegevensverwerking**) (zie hier voor meer informatie op p. 12);
- De persoonsgegevens dienen **juist** te zijn en **geactualiseerd** en indien nodig gewist of gecorrigeerd mits redelijke maatregelen (zie hier voor meer informatie op p. 11);
- Persoonsgegevens **niet langer dan strikt nodig te bewaren** en te anonimiseren van zodra mogelijk (zie hier voor meer informatie op p. 12);
- Passende technische en organisatorische maatregelen nemen ter verzekering van **integriteit en vertrouwelijkheid**;
- De verantwoordelijke dient de naleving van de bovenvermelde verplichtingen kunnen **aantonen** (**verantwoordingsplicht**).

II. Specifieke verplichtingen om persoonsgegevens op een veilige en gepaste manier te verwerken

- Bepalen van de **verwerkingsgrond** en uitzonderingsgrond voor gevoelige persoonsgegevens;
- **Gedetailleerde informatieverplichting**;
- Een **verwerkingsregister** bijhouden (zie hier voor meer informatie op p.15);
- Technische en organisatorische maatregelen treffen om persoonsgegevens gepast te **beveiligen** (zie hier voor meer informatie op p. 13 en concrete richtlijnen);
- **Verwerkersovereenkomst** afsluiten met verwerkers (zie hier voor meer informatie op p. 19);
- **Gegevensbeschermingseffectbeoordeling** uit te voeren indien nodig (zie hier voor meer informatie op p. 17);
- Persoonsgegevens **niet exporteren** uit de Europese Economische Ruimte tenzij gepaste maatregelen werden genomen (zie hier voor meer informatie op p. 20);
- **Melden van een gegevenslek** aan de GBA en eventueel ook aan betrokkenen (zie hier voor meer informatie op p. 29);
- Een **Gegevensbeschermingsfunctionaris** (DPO) aanstellen indien nodig (zie hier voor meer informatie op p. 16).

III. Specifieke verplichtingen ten aanzien van betrokkenen (Art. 12-25 AVG)

- Transparantie en een gedetailleerde **informatieplicht** ten aanzien van betrokkenen (zie de vraag 5 en volgende hieronder).
- Naleving van de rechten van betrokkenen, namelijk:
  - Recht op inzage;
  - Recht op rectificatie en wissen van gegevens (zie hier voor meer informatie op p. 25);
  - Recht op beperking van de verwerking van gegevens (zie hier voor meer informatie op p. 26);
  - Recht op gegevensoverdraagbaarheid (zie hier voor meer informatie op p. 27);
  - Recht van bezwaar (zie hier voor meer informatie op p. 26);
  - Recht om niet aan geautomatiseerde besluitvorming onderworpen te worden (zie hier voor meer informatie op p. 28).

5. WAT IS HET TRANSPARANTIEBEGINSEL ONDER DE AVG EN WELKE INFORMATIE MOET IK MEEDELEN?

De AVG wil meer controle geven aan betrokkenen over de verwerking hun persoonsgegevens. Een van de belangrijke instrumenten voor controle is in de eerste plaats transparantie, waaronder het informeren van betrokkene(n) van elk gebruik en verwerking van deze persoonsgegevens. Slechts indien het gebruik van persoonsgegevens 'transparant' is voor betrokkenen, kunnen zij eventuele risico's inschatten en beslissingen nemen over hun persoonsgegevens.

De AVG verplicht verwerkingsverantwoordelijken dus om informatie te verlenen aan betrokkenen over de identiteit van de verantwoordelijke en welke persoonsgegevens ze verzamelen, hoe ze deze gebruiken (bijv. ook om profielen aan te maken, te volgen op websites, ...) en aan wie dit doorgegeven wordt, hoe lang deze bewaard worden, etc. Daarenboven hebben betrokkenen diverse rechten, waaronder het recht om informatie op te vragen over en inzage te krijgen (Artikel 15 AVG) in de verwerking van hun persoonsgegevens (zie ook hieronder).

Wettelijke basis: Artikel 12 en volgende AVG

Voor meer informatie zie de richtlijnen omtrent transparantie van de Werkgroep 29

WIE ZIJN DE 'BETROKKENEN'?

Betrokkenen zijn de individuele personen van wie U de persoonsgegevens verwerkt. Ondernemingen en bedrijven zijn geen betrokkenen, noch overleden personen.

Wettelijke basis: Artikel 4, (1) AVG

Voorbeelden van betrokkenen zijn: de werknemers waarvan de loonfiche wordt opgesteld, de persoon waarvan een foto wordt opgeslagen, de klanten die zich bevinden op een klantenlijst, de houders van een telefoonnummer of e-mailadres dat wordt gebruikt voor marketing, de persoon waarvan localisatiegegevens worden opgeslagen en/ of doorgestuurd, ...

6. WAT IS EEN 'PRIVACYVERKLARING'?

Ondernemingen moeten bij *rechtstreekse inzameling* bij betrokkenen gedetailleerde informatie over de verwerkingen aan betrokkenen communiceren op een **beknopte, transparante, begrijpelijke** manier, in een **gemakkelijk toegankelijke** vorm en in **duidelijke en eenvoudige taal**. Dit kan schriftelijk (bijvoorbeeld op de keerzijde van een offerte) of op elektronische wijze (bijv. op een website). Indien de betrokkene dit vraagt, kan U deze informatie ook mondeling verschaffen, maar dan moet U dit nadien wel kunnen bewijzen.

Zelfs bij *onrechtstreekse inzameling,* dus indien U de persoonsgegevens **niet rechtstreeks van een betrokkene zelf ontvangt**, maar bijvoorbeeld via een derde partij, moet u dezelfde gedetailleerde informatie aan betrokkenen verstrekken, met daar bovenop de categorieën van persoonsgegevens en de bron daarvan, tenzij de betrokkenen bijvoorbeeld de informatie reeds heeft of dit onmogelijk of onevenredig veel inspanning zou vergen.

Voorbeeld: Persoonsgegevens gekocht van een handelaar *(data broker)*, verzameld op sociale media, verkregen via een andere onderneming of platform, ...

Wettelijke basis: Artikel 12 en de Artikelen 13 en 14 AVG

Voor meer informatie zie de richtlijn omtrent transparantie van de Werkgroep 29.

WELKE CONCRETE TIPS KAN IK GEBRUIKEN BIJ HET OPSTELLEN EN COMMUNICEREN VAN EEN PRIVACYVERKLARING?

- *Bepaal* voor elke categorie van betrokkenen (bijv. leveranciers, klanten, werknemers, bezoekers website, ...) *waar* de privacyverklaring omtrent de verwerkingen die hen betreffen, zal geplaatst worden (bijv. keerzijde offertes, arbeidsovereenkomst, website);
- Zet indien relevant (bijv. voor bezoekers van de website, gebruikers van een online product, bezoekers van evenementen, ...) een privacyverklaring op Uw *website* die informeert over de relevante persoonsgegevensverwerkingen van Uw bedrijf voor deze betrokkenen (zowel online als offline). Plaats vervolgens een *link* naar de privacyverklaring op de hoofdpagina én elke volgende pagina van de website zodat deze makkelijk teruggevonden kan worden;
- Maak een *vertaling* van de privacyverklaring beschikbaar in alle talen van de website;
- Hang een *poster* van de privacyverklaring uit, op een publiek toegankelijke plaats voor relevante betrokkenen (bijv. bezoekers van een winkel) ;
- Stem het taalgebruik van de verklaring af op het publiek:
  - Gebruik geen passieve werkwoorden;
  - Vermijd complexe woorden en te lange zinconstructies;
  - Werk met een tekst 'in meerdere lagen' van detail en complexiteit (d.i. bijv. met hyperlinks die toelaten door te klikken, een samenvatting en daarachter een meer uitgebreide versie indien nodig, ...);
  - Indien U persoonsgegevens verkregen bij kinderen verwerkt, moet de privacyverklaring begrijpelijk zijn voor de leeftijd van het kind;
- Dateer de privacyverklaring en update deze regelmatig in functie van de (gewijzigde) verwerkingen. Houd deze verschillende versies bij; en
- Gebruik onze onderstaande checklist om geen verplichte vermeldingen te vergeten.

WANNEER MOET U EEN 'PRIVACYVERKLARING' MEEDELEN?

Wanneer U de gegevens **rechtstreeks** van de betrokkene verkrijgt, dient U deze informatie **vooraf** mee te delen en uiterlijk **wanneer U de persoonsgegevens verzamelt**.

Wanneer U de gegevens **niet rechtstreeks** van de betrokkene verkrijgt, dient U de privacyverklaring mee te delen:

- Ten laatste *binnen een maand* nadat U de persoonsgegevens verkregen hebt;
- Wanneer U deze persoonsgegevens verkrijgt om de betrokkene te contacteren, *op het moment van dat eerste contact*; of
- Wanneer U deze persoonsgegevens wenst te delen met een andere onderneming, ten laatste wanneer deze gegevens *voor het eerst gedeeld worden.*

WAT MOET U COMMUNICEREN OM VOLDOENDE TRANSPARANT TE ZIJN?

Indien u, als verwerkingsverantwoordelijke, persoonsgegevens betreffende een **betrokkene ontvangt**, moet U minstens de informatie in de onderstaande checklist communiceren aan deze betrokkene voor (het geheel van) de persoonsgegevensverwerkingen. Daarenboven kan het nodig zijn bijkomend over de risico's te informeren.

Privacyverklaring checklist bij rechtstreeks verkrijging bij betrokkenen:

U kan de vakjes aankruisen wanneer U ze toegevoegd heeft aan Uw privacyverklaring.

- ☐ de *identiteit en de contactgegevens* (bijv. naam, adres, ...) van de verwerkingsverantwoordelijke (of vertegenwoordiger indien in het buitenland);
- ☐ contactgegevens (bijv. een DPO-e-mailadres) van de functionaris voor de gegevensbescherming (DPO), indien deze werd aangesteld;
- ☐ de verwerkingsdoeleinden en de precieze rechtsgrond (bijv. toestemming, noodzaak voor uitvoering van de overeenkomst, gerechtvaardigd belang, ...) voor de verwerking, en indien die rechtsgrond het gerechtvaardigd belang, is een (korte) precisering van dat belang;
- ☐ wanneer de persoonsgegevens worden doorgestuurd, de ontvangers of categorieën van ontvangers van de persoonsgegevens (bijv. een website ontwikkelaar, het sociaal secretariaat, ...);
- ☐ indien de persoonsgegevens (zullen) worden doorgegeven buiten de Europees Economische Ruimte: of er een adequaatheidsbesluit bestaat dan wel welke waarborgen er zijn (bijv. een contract 'dat een adequaat beschermingsniveau biedt', zoals bijvoorbeeld de standard contractual clauses, ...) en waar dit geraadpleegd dan wel kopie van kan worden verkregen;
- ☐ de bewaringstermijn van de persoonsgegevens, of indien deze niet vast bepaald is, de criteria die deze bewaringstermijn bepalen (bijv. termijnen opgelegd door boekhoudwetgeving, ...);
- ☐ de precieze rechten van betrokkene;
- ☐ dat de betrokkene steeds het recht heeft zijn toestemming in te trekken;
- ☐ dat de betrokkene het recht heeft *klacht in te dienen* bij een toezichthoudende autoriteit;
- ☐ of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is,

of noodzakelijk en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;

- ☐ het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica en het belang en de gevolgen van die verwerking voor de betrokkene;

- ☐ de (categorieën van) gegevens en de (openbare) bron waar de persoonsgegevens vandaan komen, indien U de persoonsgegevens niet van de betrokkene rechtstreeks heeft ontvangen.

7. WAT MOET IK DOEN WANNEER EEN BETROKKENE VRAAGT HOE IK ZIJN PERSOONSGEGEVENS VERWERK?

Ondernemingen die verwerkingsverantwoordelijke zijn, moeten betrokkenen informeren over hun rechten onder de AVG, waaronder het recht op inzage. Dit recht op inzage betekent dat een betrokkene kan vragen aan een onderneming (i) *of* die onderneming persoonsgegevens van die betrokkene verzamelt of gebruikt en (ii) *welke*. Indien dit het geval is, moet deze onderneming meedelen *welke* persoonsgegevens van die betrokkene worden verwerkt en toegang verlenen tot deze persoonsgegevens, meer bepaald door mededeling van een *kopie* van zijn of haar persoonsgegevens, gratis, samen met de vereiste toelichting. Mededeling van de kopie gebeurt op een gangbare elektronische wijze als de betrokkene een elektronisch inzageverzoek (bijvoorbeeld via e-mail) indient, tenzij deze om een andere regeling vraagt (Art. 15 AVG). Meer informatie over dit recht tot inzage kan U hier vinden.

HOE ANTWOORD IK OP EEN VERZOEK TOT INZAGE?

U dient te antwoorden aan de betrokkene zo snel mogelijk en uiterlijk binnen een maand na ontvangst van het inzageverzoek. Deze termijn kan met twee maanden worden verlengd indien nodig wanneer het verzoek complex is of bij vele verzoeken. Dergelijke verlenging moet eveneens binnen een maand meegedeeld worden.

U dient deze informatie gratis te verschaffen.

Indien u beroep doet op een verwerker, dient U best met de verwerker af te spreken om dergelijke verzoeken binnen een bepaalde termijn (bijv. vijf werkdagen) aan u, de verwerkingsverantwoordelijke, alvast door te sturen.

Wettelijke basis: Artikelen 12 en 15 AVG

8. KAN IK PERSOONSGEGEVENS ENKEL VERWERKEN MET DE TOESTEMMING VAN DE BETROKKENE?

De verwerking van persoonsgegevens is toegestaan indien er een wettelijke grondslag voor is. Er bestaan echter naast de vrije, specifieke en geïnformeerde toestemming, diverse andere verwerkingsgrondslagen.

Het vragen van toestemming is met andere woorden slechts één mogelijke grondslag en slechts nodig wanneer een onderneming zich op geen andere wettelijke grondslag kan baseren.

Indien U zich op een andere grondslag dan toestemming, kan beroepen, vraagt U beter niet de toestemming. Dit omdat toestemming steeds kan ingetrokken worden (Art. 7.3 AVG).

HOE VERKRIJG IK EEN GELDIGE TOESTEMMING?

Om van een geldige toestemming te kunnen spreken moet deze:

- vrij worden gegeven;
- specifiek zijn;
- geïnformeerd zijn; en
- ondubbelzinnig zijn.

Opgelet: Wanneer een betrokkene (bijv. een werknemer) *geen andere keuze* heeft dan toestemmen, is de toestemming niet geacht vrij te zijn en bijgevolg doorgaans ongeldig. De betrokkene moet ook *vooraf* een goede omschrijving krijgen van het doel van de verwerking, zodat de betrokkene een geïnformeerde keuze kan maken over het al dan niet geven van de toestemming. Verder dient de toestemming in bepaalde gevallen eveneens een *ondubbelzinnige actieve handeling* zijn (aangevinkte hokjes zijn uit den boze) of verklaring (Art. 4(11) AVG). Zolang de verwerking loopt, moet de verwerkingsverantwoordelijke kunnen aantonen dat een geldige toestemming is verkregen.

Opgelet: De toestemming moet eveneens zichtbaar *afzonderlijk gevraagd worden en dus onderscheiden* worden van de toestemming die eventueel gevraagd wordt voor andere gelegenheden (bijv. toestemming met algemene voorwaarden): dit kan door de toestemming bijvoorbeeld in een duidelijk kader onder deze voorwaarden te plaatsen of in een apart scherm. De toestemming voor gegevensverwerkingen *mag ook niet gekoppeld worden* aan de toestemming voor uitvoering van een overeenkomst (bijv. toestemming voor het downloaden van een applicatie, ….), en moet dus afzonderlijk gevraagd worden.

Wettelijke basis: Artikelen 4(11) en 7 AVG

Voor meer informatie zie de richtlijn 5/2020 omtrent toestemming van de EDPB.

DE GESCHILLENKAMER OVER EEN SOCIAAL NETWERKPLATFORM EN TOESTEMMING

De Geschillenkamer legde een boete op van 50.000 euro aan een internationaal sociaal netwerk voor het verzamelen en gebruik van persoonsgegevens in het kader van een functie 'contacten uitnodigen'. Hiermee konden lid-gebruikers van het sociaal netwerk op het platform contacten uitnodigen (ongeacht of zij al lid-gebruiker zijn) en verzamelde en bewaarde het sociaal netwerk enerzijds gegevens betreffende de contacten en anderzijds stuurde zij uitnodigingen naar de personen die door de gebruiker werden toegevoegd.

De Geschillenkamer stelde onder meer de volgende inbreuken op de AVG vast:

- **Ontbreken van de toestemming** van de betrokken personen die geen lid-gebruiker

zijn van het netwerk: de toestemming van het lid-gebruiker volstaat niet om de gegevens te verwerken van de niet-leden. Het netwerk verwerkte dus de persoonsgegevens zonder geldige rechtsgrond (inbreuk op artikel 6 van de AVG);

- De toestemming van het lid-gebruiker van het netwerk dat zijn contacten wilde uitnodigen was **dus niet geldig omdat tijdens het proces om de contacten toe te voegen, de vakjes vooraf aangevinkt waren** (inbreuk op de artikelen 4(11) en 7 van de AVG). Deze praktijk is in strijd met de toestemmingsvoorwaarden zoals bedoeld in de AVG, deze moet immers vrij zijn en vereist een positieve en duidelijke actie: de betrokken persoon moet dus zelf de gewenste vakjes aanvinken.

Lees de volledige beslissing van 14 mei 2020 van de Geschillenkamer hier.

9. MOETEN KMO'S EEN VERWERKINGSREGISTER BIJHOUDEN?

Elke onderneming die persoonsgegevens verwerkt (behoudens de uitzondering hieronder) dient in principe een verwerkingsregister bij te houden van alle verwerkingsactiviteiten die onder haar verantwoordelijkheid valt. Dit register is een soort inventaris van alle verwerkingen van persoonsgegevens en is nuttig om een correcte inschatting te maken van de AVG verplichtingen en eventuele risico's.

U vindt hier een voorbeeld van verwerkingsregister in de vorm van een elektronisch invulbestand (in het Engels) gepubliceerd door de Franse gegevensbeschermingsautoriteit (CNIL) dat U kan gebruiken voor het register van Uw onderneming.

Merk op dat voor ondernemingen die *minder dan 250 personen* tewerk stellen, een register evenwel *niet* vereist is. De draagwijdte van deze uitzondering is echter beperkt aangezien ze niet geldt wanneer het gaat om risicovolle verwerkingen, verwerkingen van gevoelige gegevens of verwerking die ingebed zijn in het dagdagelijkse functioneren van de onderneming zoals personeels-, klanten- en leveranciersbeheer. Indien U twijfelt of U al dan niet onder deze uitzondering valt, raden wij u aan om toch een - weliswaar simpel - register bij te houden.

Elke onderneming dient **alle verwerkingen regelmatig te evalueren**, en het register indien nodig aan te vullen of aan te passen.

Wettelijke basis: Artikel 30 AVG

Voorbeeld 1: Een KMO met vijf personeelsleden beheert een platform voor het delen van radiografieën van patiënten en andere gegevens. Dit zijn 'gevoelige' gegevens. Een register is vereist.

Voorbeeld 2: Een éénmansmarketingbedrijf 'verkoopt' e-mailgegevens en bijhorende

profiel(click)data aan derden. De inzameling, opslag en mededeling aan derden van deze persoonsgegevens is geen bijkomstige maar hoofdactiviteit. Een register is vereist.

10. WAT KAN MEN DOEN INDIEN EEN VERWERKER GEEN VERWERKINGSOVEREENKOMST WIL ONDERTEKEN?

De ondertekening van een verwerkingsovereenkomst tussen de verantwoordelijke en de verwerker(s) is altijd verplicht.

Wettelijke basis: Artikel 28.3 AVG

Om dit af te dwingen, vindt U hieronder enkele tips:

- U kan de modelverwerkersovereenkomst gepubliceerd door de Deense gegevensbeschermingsautoriteit (ook beschikbaar in het Nederlands en Frans) als leidraad gebruiken;
- U kan aangeven dat de ondertekening van een verwerkersovereenkomst een wettelijke verplichting is voor beide partijen en dat de GBA optreedt tegen verwerkingsverantwoordelijken die geen verwerkingsovereenkomst afsluiten (zie de beslissing hieronder);
- U bepaalt bijv. in de hoofdovereenkomst met de IT-leverancier dat de verwerkingsovereenkomst integraal deel uitmaakt van de overeenkomst tussen partijen en voegt als verantwoordelijke Uw contractvoorstel toe als bijlage bij de te ondertekenen hoofdovereenkomst;
- U bepaalt in de hoofdovereenkomst dat ondertekening van een afzonderlijke verwerkersovereenkomst verplicht is en betaling van prestaties kan worden opgeschort tot ondertekening van de verwerkersovereenkomst.

DE GESCHILLENKAMER OVER DE VERPLICHTING TOT HET SLUITEN VAN EEN VERWERKERSOVEREENKOMST

De verwerkingsverantwoordelijke meldde bij de GBA een gegevenslek, dat had plaatsgevonden in het kader van een verwerking van persoonsgegevens door een verwerker in India. Het lek had plaats na een verwerking die niet door de verwerkingsverantwoordelijke was toegestaan en die uitdrukkelijk was verboden in de verwerkersovereenkomst tussen de partijen.

De Geschillenkamer benadrukte dat de verwerkingsverantwoordelijke *proactief* passende

technische en organisatorische maatregelen moet nemen om een passend veiligheidsniveau te waarborgen (artikelen 5.1 f), en 24.1 van de AVG) en dat de verwerkingsverantwoordelijke moet kunnen aantonen op een transparante wijze dat er maatregelen werden genomen (beginsel van de verantwoordingsplicht opgenomen in artikel 5.2 van de AVG).

De Geschillenkamer merkte op hoe belangrijk het is dat de verwerkingsverantwoordelijke nauwgezet omgaat met de formulering en de opvolging van een dergelijke verwerkingsovereenkomst en de vervulling van alle wettelijke verplichtingen dienaangaande (zoals vermeld in artikel 28.3 van het AVG). Ze beschouwt dit als een **resultaatsverbintenis**.

Lees de volledige beslissing van 8 mei 2020 van de Geschillenkamer hier.

11. WAT IS EEN GEGEVENSBESCHERMINGSEFFECTBEOORDELING (GEB) EN WANNEER IS DEZE VERPLICHT?

De verschillende niveaus van bescherming die de AVG wil brengen zijn gebaseerd op een risicoanalyse. Dit betekent dat ondernemingen die verwerkingsverantwoordelijke zijn in bepaalde gevallen verplicht zijn een formele risicoanalyse, namelijk een GEB, uit te voeren.

Ondernemingen moeten in het algemeen deze GEB uitvoeren wanneer het verzamelen en/of gebruiken van persoonsgegevens *waarschijnlijk een groot risico inhoudt voor de rechten en vrijheden* van betrokkenen, zoals bijvoorbeeld het recht op vrije meningsuiting, op privacy, … Het gebruiken van persoonsgegevens *houdt in het bijzonder een groot risico in* i) bij geautomatiseerde *besluitvorming* over betrokkenen op basis van een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, met rechtsgevolgen of die hen wezenlijk treffen (bijv. bij het opmaken van profielen), ii) het verzamelen en gebruiken van gevoelige persoonsgegevens op *grote schaal* (bijv. medische gegevens), en iii) het stelselmatig en grootschalig *monitoren* van openbare ruimten (bijv. via camerabewaking).

U vindt hier een software tool (in het Engels) gepubliceerd door de Franse gegevensbeschermingsautoriteit (CNIL) die U kan gebruiken voor het uitvoeren van een GEB voor Uw onderneming.

Wettelijke basis: Artikel 35 AVG. Meer informatie vindt u eveneens hier.

Voorbeeld 1: Persoonsgegevens worden geconsulteerd bij derden om vervolgens in aanmerking te worden genomen bij de beslissing om een welbepaalde dienstverleningsovereenkomst met een natuurlijke persoon te weigeren of stop te zetten (bijv. verzekeringskantoor dat een RSR-databank of 'zwarte lijst' raadpleegt vooraleer de consument een definitief verzekeringsvoorstel te doen). De onderneming/ KMO moet een GEB uit voeren.

Voorbeeld 2: Gezondheidsgegevens van patiënten worden op geautomatiseerde wijze ingezameld aan de hand van actieve inplantbare medische voorzieningen (bijv. meten en aanpassen bloedsuikerspiegel via de chip) die gebruikt worden op grote schaal. De onderneming/ KMO moet een GEB uit voeren.

Voorbeeld 3: Wanneer grootschalige verwerking van gegevens, gegenereerd via bijv. slimme armbandjes of toestellen met sensoren die via het internet of ander medium gegevens versturen (internet-of-things toepassingen), wordt gebruikt voor gedragsanalyse of profilering (bijv. smartTV die voorkeuren analyseert en voorstellen van tv-programma's doet), dient de onderneming een GEB uit te voeren.

Voorbeeld 4: Een KMO die gebruik maakt van een online wervingsplatform dat op basis van een automatische lezing van het CV, kandidaten automatisch selecteert of afwijst, dient een GEB uit te voeren.

Voorbeeld 5: Een KMO observeert het surfgedrag van personeelsleden stelselmatig om overmatig privégebruik tijdens de werkuren te voorkomen. De werknemers bevinden zich in een ondergeschikte positie en het risico is hoog. Bijgevolg dient de onderneming een GEB uit te voeren.

WAT ZIJN GEVOELIGE PERSOONSGEGEVENS?

'Gevoelige' persoonsgegevens zijn:

- **persoonsgegevens waaruit het volgende blijkt:**
  - ras of etnische afkomst;
  - politieke opvattingen;
  - religieuze of levensbeschouwelijke overtuigingen;
  - lidmaatschap van een vakbond;

- **verwerkingen van genetische gegevens;**
- **verwerkingen van biometrische gegevens met het oog op de unieke identificatie van een persoon;**
- **gegevens over gezondheid;**
- **gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.**

Het **verwerken** van deze gegevens is **in principe verboden**, tenzij er aan zeer specifieke voorwaarden wordt voldaan.

Wettelijke basis: Artikel 9 AVG

Voorbeeld: medische fiches, locatiegegevens waaruit blijkt dat een persoon elke zondag voor de kerk of moskee parkeert gedurende twee uur, doktersbriefje, ...

WAT ZIJN ANONIEME GEGEVENS?

Anonieme gegevens zijn gegevens waarbij het niet meer mogelijk is om een individu te identificeren of identificeerbaar te maken. Dan is de **AVG en de Gegevensbeschermingswet 2018 niet van toepassing**. De technologische vooruitgang heeft ervoor gezorgd dat veel gegevens die anoniem lijken toch persoonsgegevens zijn, omdat ze natuurlijke personen toch kunnen identificeren door ze te combineren met andere persoonsgegevens.

Het **pseudonimiseren** of **versleutelen** van persoonsgegevens zijn veiligheidsmaatregelen die het moeilijker maken voor onbevoegden (bijv. hackers) om de persoonsgegevens te lezen of in verband te brengen met personen. In dit geval blijft de **AVG en de Gegevensbeschermingswet 2018 wel van toepassing**.

Wettelijke basis: Overweging 26 AVG

Voor meer informatie zie de Werkgroep 29 Opinie 05/2014 omtrent het anonimiseren van data.

12. DIENT MIJN ONDERNEMING EEN GEGEVENSBESCHERMINGSFUNCTIONARIS (DATA PROTECTION OFFICER (DPO)) AAN TE STELLEN?

Een onderneming, zowel een verantwoordelijke als verwerker, dient *verplicht* een DPO aan te stellen indien haar taken *hoofdzakelijk* bestaan uit het regelmatig en systematisch monitoren *op grote schaal* van betrokkenen en/of verwerken van 'gevoelige' persoonsgegevens *op grote schaal*. In alle andere gevallen *blijft een DPO een aanrader, maar is niet verplicht.*

Wie mag de rol opnemen van DPO? Een bestaande werknemer met voldoende kennis inzake AVG (indien de professionele taken van de medewerker compatibel zijn met deze van de DPO en dit niet leidt tot belangenconflicten) of een externe persoon. De DPO moet zijn taken dus onafhankelijk kunnen uitoefen en moet rechtstreeks verslag kunnen uitbrengen aan het hoogste management.

Let daarom goed op de gevallen waarin de aanwijzing van een DPO verplicht is (artikel 37.1 van de AVG) en zorg er in voorkomend geval voor dat deze persoon in staat is zijn of haar functie in alle onafhankelijkheid en met kennis te vervullen (zie ook artikel 38 van de AVG).

Voorbeeld: De bestuurder van een vennootschap kan niet de DPO zijn van deze vennootschap, aangezien de DPO onafhankelijk moet zijn. Deze bestuurder kan niet onafhankelijk zijn, aangezien zij/ hij de belangen van de vennootschap nastreeft.

Wettelijke basis: Artikel 37 en volgende AVG

Voor meer informatie zie de richtlijn omtrent gegevensbeschermingsfunctionarissen van de Werkgroep 29 en de GBA's themadossier.

DE GESCHILLENKAMER OVER DE FUNCTIE VAN DE DPO

De Geschillenkamer legde een boete op van 50.000 euro voor het niet naleven van de verplichting met betrekking tot de functie van DPO.

Krachtens artikel 38.6 van de AVG, kan de DPO andere opdrachten en taken vervullen maar op voorwaarde dat deze **geen belangenconflicten** veroorzaken. De Geschillenkamer stelde vast dat een onderneming deze verplichting niet naleefde omdat de rol van DPO werd uitgeoefend door de '*Head of the Compliance, Risk Management and Audit department*'. De Geschillenkamer oordeelde onder meer dat de combinatie van deze twee functies het onafhankelijk toezicht van de DPO belemmert op de verwerking van persoonsgegevens die wordt verricht door het departement '*Compliance, Risk Management and Audit*'.

Lees de volledige beslissing van 28 april 2020 van de Geschillenkamer hier.

13. HOE BLIJF IK OP DE HOOGTE VAN DE ONTWIKKELINGEN VAN DE AVG?

U kan op de hoogte blijven van de ontwikkelingen op nationaal (en ook Europees) vlak door regelmatig de website van de GBA te consulteren met specifieke zoektermen en bijvoorbeeld door U te abonneren op de tweemaandelijkse nieuwsbrief van de GBA voor KMO's in het kader van het BOOST-project.

14. WAT ZIJN DE SANCTIES INDIEN MIJN ONDERNEMING DE AVG NIET NALEEFT OF OVERTREEDT?

Wanneer Uw onderneming de AVG niet naleeft, kan de GBA U onder andere een administratieve boete opleggen, maar ook verwerkingen beperken of verbieden. Bovendien kan Uw onderneming veroordeeld worden door een rechtbank tot het staken van onwettige praktijken en/of het betalen van een schadevergoeding. Er kunnen eveneens strafsancties opgelegd worden.

Wettelijke basis: Artikel 83 AVG en Artikel 209 en volgende Gegevensbeschermingswet 2018

Meer informatie vindt U in onze brochure Wegwijs in de AVG voor KMO's op p. 30.

15. WELKE VERPLICHTINGEN DIEN IK NA TE LEVEN INDIEN IK COOKIES GEBRUIK ?

Cookies zijn 'minibestanden' die geplaatst worden (bijv. bij de ontwikkeling van een applicatie of een website) op apparatuur van een gebruiker die is verbonden met het internet, zoals een computer, telefoon, tablet of smartTV. Cookies verzamelen vaak persoonsgegevens. Bijgevolg is o.a. de AVG van toepassing.

Let eveneens op bij het plaatsen van social media-plug-ins op uw website, zoals bijv. een Facebook Like-button. Het EHvJ bepaalde in haar arrest Fashion ID dat een onderneming die een dergelijke like button op haar website heeft geplaatst gezamenlijk verantwoordelijk is met de sociale media-aanbieder.

U vindt meer informatie over de informatie- en andere verplichtingen bij het gebruik van cookies op deze GBA website pagina.