KLAAR VOOR DE AVG
IN 10 STAPPEN

LEGENDA: WIE TE BETREKKEN?

L Leidinggevenden
J Juridisch of compliance team
HR HR
IT IT
S Sales en marketing
A Accounting en finance
O Overige verwerkers van persoonsgegevens
E Externe adviesverleners

1 Bewustmaking van de organisatie van persoonsgegevens en de AVG

De AVG legt verplichtingen op met betrekking tot persoonsgegevens die rechtstreeks de werking van een organisatie kunnen beïnvloeden.

Indien jij nog niet eerder hebt gehoord van de AVG of jouw organisatie hier nog niets heeft rond gedaan, kan je meerdere zaken doen:

- Contacteer de leidinggevenden en bedrijfsjuristen en wijs hen op het belang van de AVG en op dit stappenplan in het bijzonder.
- Ga na of sectororganisaties relevante en specifieke AVG documentatie aanbieden. Deze kunnen een goed hulpmiddel zijn.
- Indien het gaat om een kleine organisatie: volg dit stappenplan en werk zo toe naar naleving van de AVG-verplichtingen.
- Schakel zo nodig externe adviesverleners in.

L J E

2 Controleer of jouw organisatie een DPO moet aanstellen en/of stel een verantwoordelijk team voor gegevensbescherming aan

Een functionaris voor gegevensbescherming of Data Protection Officer (DPO) houdt zich bezig met het implementeren en monitoren van de naleving van de AVG-verplichtingen binnen een organisatie.

Sommige organisaties moeten een DPO aanstellen, bijvoorbeeld:
- openbare overheden
- organisaties wiens kerntaak bestaat uit het regelmatig en stelselmatig observeren op grote schaal van personen of een grootschalige verwerking van gevoelige gegevens

Laat de juristen of externe adviseurs verifiëren of dit nodig is. Zorg er ook voor dat een eventuele beslissing op papier wordt gezet.

Niettemin is het aan te raden om ook indien dat niet strikt verplicht is iemand of een team aan te duiden met een gelijkaardige verantwoordelijkheid als die van een DPO.

- Bepaal welke plaats een (externe) DPO of gelijkaardige functie inneemt binnen de organisatie. Daarbij dient verzekerd te worden dat een DPO de kennis, medewerking en bevoegdheid heeft om zijn/haar taken te volbrengen.
- Stel een team samen met een projectleider - al dan niet de aangestelde DPO - om jouw organisatie door de AVG-oefening te leiden. Zorg voor een duidelijke taakverdeling.

L J HR IT E

3 Breng gegevensstromen in kaart, stel een register van verwerkingsactiviteiten op en evalueer de rechtsgrond van verwerkingen (incl. de wijze waarop toestemming wordt gevraagd)

Stap 1: Welke verwerkingsactiviteiten zijn er?
Breng in kaart welke afdelingen welke persoonsgegevens verwerken. Gestandaardiseerde vragenlijsten kunnen helpen om te peilen naar:
- de reden waarvoor persoonsgegevens gebruikt worden
- de bronnen van de persoonsgegevens
- de locatie waar ze opgeslagen zijn
- of en aan wie ze worden doorgegeven.

Stap 2: Stel een verwerkingsregister op
De ingevulde vragenlijsten zullen een goede basis vormen om het register van verwerkingsactiviteiten op te stellen. Eventueel kan je dit combineren met een meer IT-gerichte informatie-audit. Om hierbij te helpen, stelt de Belgische Gegevensbeschermingsautoriteit (GBA) een modelregister van verwerkingsactiviteiten ter beschikking op haar website met een bijbehorende handleiding.

Stap 3: Welke rechtsgrond?
Na de eerste stappen is het belangrijk om te bepalen op basis van welke rechtsgrond de persoonsgegevens verwerkt worden.

De AVG voorziet zes gronden, waaronder toestemming. Baseer je je op deze rechtsgrond, ga dan na of de toestemming wel correct werd gevraagd en verkregen. Het verwerken van persoonsgegevens zonder rechtsgrond vormt een risico en moet herbeoordeeld worden.

Deze stap zal tijd in beslag nemen, maar het is belangrijk dat deze op een goede manier wordt uitgevoerd. Een overzichtelijk register zal ervoor zorgen dat alle volgende stappen vlotter verlopen.

J HR IT S A O E

KLAAR VOOR DE AVG
IN 10 STAPPEN

4 Bereid je voor op het behandelen van verzoeken van betrokkenen procedures

Onder de AVG hebben personen een aantal rechten die ze kunnen uitoefenen, o.a. het recht op informatie en toegang tot hun persoonsgegevens, correctie en wissing van persoonsgegevens.

- Stel interne procedures op om te kunnen reageren op dergelijke verzoeken (bijv. door draaiboeken met de nodige procedures en stappenplannen op te stellen, de verantwoordelijken hiervoor aan te duiden en indien nodig de systemen aanpassen).
- De antwoordtermijn is in principe één maand, maar kan in bepaalde gevallen verlengd worden met twee maanden

In specifieke gevallen kunnen verzoeken geweigerd worden, maar deze moeten door de organisatie gemotiveerd worden.

Vermeld ook telkens dat iemand het recht heeft om klacht in te dienen bij de GBA en de mogelijkheid heeft om beroep bij de (burgerlijke) rechter in te stellen.

J IT E

5 Bepaal welke toezichthoudende autoriteit bevoegd is in het geval van internationale activiteiten. Controleer ook of derde landen voldoende bescherming bieden.

Een internationaal bedrijf met hoofdzetel in België valt onder de bevoegdheid van de GBA. Waar de hoofdvestiging ligt of waar de beslissingen omtrent het verwerken van persoonsgegevens worden genomen, bepaalt de leidende bevoegde autoriteit.

Indien persoonsgegevens doorgegeven worden aan landen buiten de Europese Economische Ruimte (EER), moet nagegaan worden of ze voldoende bescherming bieden. Er zijn verschillende mogelijkheden:

- Adequaatheidsbesluit: Europese Commissie heeft onderzocht of een derde land een passend beschermingsniveau biedt. De lijst van landen vindt men hier terug.
- De modelcontractbepalingen van de Europese Commissie kunnen gebruikt worden. Deze mogen in principe niet veranderd worden tenzij in de voorziene rubrieken.
- Eigen overeenkomsten kunnen ook, maar dan moeten ze ter goedkeuring aan de bevoegde toezichthoudende autoriteit voorgelegd worden.

Opgelet: veel contracten verwijzen naar het mechanisme van het Amerikaanse Privacy Shield, maar dit werd in juli 2020 ongeldig verklaard, omdat het te weinig waarborgen bood voor de Europese persoonsgegevens.

J IT E

6 Zet een (voorlopige) privacy- en cookieverklaring op jouw site of pas die aan. Pas alle relevante documenten aan indien nodig.

Personen moeten weten of en waarom hun persoonsgegevens verwerkt worden. Dit kan via verschillende documenten (o.a. privacy- & cookieverklaring, vacatures, formulieren, nieuwsbrieven en e-mails).

Het gaat om de volgende informatie: wie verwerkt; welke gegevens; waarom; welke rechtsgrond; bewaartermijnen; eventuele ontvangers; eventuele internationale doorgiften; welke rechten er zijn; toepassen geautomatiseerde besluitvorming en/of profiling; eventueel gegevens DPO.

Ga na of bestaande documenten deze informatie of de nodige links al bevatten.

Gebruik eenvoudige en begrijpelijke taal en zorg dat de informatie gemakkelijk beschikbaar is.

In het geval van direct marketing (bijv. nieuwsbrieven, mailings) zorg ervoor dat de bestemmeling zich altijd gemakkelijk kan uitschrijven (bijv. via een unsubscribe-button).

J HR IT S E

7 Pas de contracten met leveranciers en klanten aan (incl. verwerkersovereenkomst)

Elke vorm van samenwerking houdt in dat er in zekere mate persoonsgegevens verwerkt worden, ook al is dit niet het hoofddoel van de overeenkomst. Daarom bevatten overeenkomsten van de organisatie best een bepaling over gegevensverwerking.

Indien een leverancier in opdracht van de organisatie persoonsgegevens verwerkt, is deze een verwerker en moet er een verwerkersovereenkomst opgesteld worden (bijv. sociaal secretariaat). Er kunnen ook persoonsgegevens doorgestuurd worden naar een andere verwerkingsverantwoordelijke (bijv. verzekeringsmaatschappij, leasemaatschappij). In dit geval moet geen verwerkersovereenkomst opgesteld worden. Het is wel aangeraden om een clausule op te nemen waarin wordt verwezen naar de plichten van de AVG en dat elke verwerkingsverantwoordelijke deze zal naleven.

- Bepaal welke rol de organisatie heeft waarnaar de persoonsgegevens worden doorgestuurd: verwerkingsverantwoordelijke of verwerker.
- Afhankelijk daarvan dient er al dan niet een verwerkersovereenkomst worden opgemaakt of dienen de contracten aangepast worden met een clausule die bepaalt dat de partijen de verplichtingen van de AVG zullen naleven.

J IT S E

Kenniscentrum
Data & Maatschappij

KLAAR VOOR DE AVG
IN 10 STAPPEN

8 Stel een intern gegevensbeleid op

De eigen medewerkers moeten de AVG ook respecteren. Bovendien moeten zij de persoonsgegevens van klanten en leveranciers ook respecteren.

Advies: stel een intern gegevensbeleid op en een privacyverklaring voor de medewerkers, met een verwijzing hiernaar in de arbeids- of dienstenovereenkomsten en het arbeidsreglement.

- De privacyverklaring ten aanzien van medewerkers bevat de informatie beschreven onder stap 6 hierboven en kan eventueel worden aangevuld met een interne klachtenprocedure.
- Het interne gegevensbeleid bepaalt hoe de medewerkers moeten omgaan met persoonsgegevens, waarom bepaalde technische en organisatorische beschermingsmaatregelen genomen moeten worden en het belang van gegevensbescherming door ontwerp bij de ontwikkeling van producten en diensten.

Bovendien is een document omtrent informatieveiligheid ook onontbeerlijk. Zeker voor organisaties die veel persoonsgegevens verwerken is een degelijk informatieveiligheidsbeleid cruciaal om datalekken te voorkomen.

Breng ook alle medewerkers op de hoogte van deze documenten door de nodige opleiding of training.

L J HR IT S A O E

9 Bereid je voor op datalekken en stel een datalek-procedure op

Een inbreuk op persoonsgegevens moet binnen de 72 uur na kennisname gerapporteerd worden aan de GBA indien er een risico is voor de rechten en vrijheden van de betrokken personen. Laat een organisatie na dit te doen en de GBA komt er toch achter, kan dit aanleiding geven tot de zwaarste boetes.

Belangrijk: stel een heldere datalek-procedure op en verspreid deze intern.

Opgelet: een datalek is niet enkel hacking, maar ook bijv. het verlies van laptop, gsm of USB-stick met persoonsgegevens.

Een datalek-procedure bevat minstens een lijst met alle personen die betrokken moeten worden; een methodologie om het risico van een datalek te bepalen en de te volgen stappen in verschillende situaties.

In het geval van een 'hoog risico' voor de rechten en vrijheden van betrokken personen (bijv. financiële verliezen), moeten die personen zelf onmiddellijk geïnformeerd worden. Modelbepalingen kunnen helpen om snel te schakelen.

Een verwerker moet eveneens onmiddellijk de verwerkingsverantwoordelijke op de hoogte brengen van het datalek.

Een datalek-register moet bijgehouden worden met telkens: de feiten, de gevolgen en de genomen maatregelen.

Beveiliging is essentieel: tref de nodige technische, organisatorische en infrastructuele maatregelen om het risico op datalekken te voorkomen. Benadruk hiervan ook het belang bij de medewerkers.

L J IT E

10 Evalueer risicovolle verwerkingsactiviteiten dmv een GEB

In geval van verwerkingsactiviteiten met een hoog risico voor de rechten en vrijheden van betrokkenen moet er een gegevensbeschermingseffectbeoordeling (GEB) worden opgesteld, bijv. bij een nieuwe technologie of indien profileringstechnieken een aanzienlijk effect kunnen hebben voor de betrokken personen.

Indien er ondanks eventuele genomen maatregelen een hoog risico blijft, moet er advies gevraagd worden aan de GBA over de wetmatigheid van de verwerking.

Stel daarom een sjabloon GEB op voor verwerkingsactiviteiten met een hoog risico. Dit bevat minstens de volgende elementen:

- Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen in het kader van het specifieke doeleinden.
- Een beoordeling van de risico's van de verwerking voor de rechten en vrijheden van de betrokken personen.
- De corrigerende maatregelen die zullen worden genomen om de bescherming van de persoonsgegevens te garanderen.

Indien een DPO aangesteld werd, moet deze in dergelijke gevallen om zijn advies worden gevraagd.

J IT E

Kenniscentrum Data & Maatschappij

Kenniscentrum Data en Maatschappij (2021). Fiche: Klaar voor de AVG in 10 stappen. Kenniscentrum Data & Maatschappij, Brussel: Kenniscentrum Data & Maatschappij.

KLAAR VOOR DE AVG
IN 10 STAPPEN

TE MAKEN DOCUMENTEN PER STAP

1 Bewustmaking van de organisatie van persoonsgegevens en de AVG

- Geen documenten

2 Controleer of jouw organisatie een DPO moet aanstellen en/of stel een verantwoordelijk team voor gegevensbescherming aan

- Schriftelijke beslissing omtrent aanstelling DPO
- Interne taakverdeling met het oog op het AVG-project

3 Breng gegevensstromen in kaart, stel een register van verwerkingsactiviteiten op en evalueer de rechtsgrond van verwerkingen (incl. de wijze waarop toestemming wordt gevraagd)

- AVG-vragenlijsten (kunnen worden opgesteld zodat zij peilen naar de informatie die vereist is in het modelregister van de GBA)
- Ingevuld register van verwerkingsactiviteiten

4 Bereid je voor op het behandelen van verzoeken van betrokkenen procedures

- Procedure om verzoeken van betrokkenen te behandelen
- Interne taakverdeling om deze verzoeken te beantwoorden en op te volgen

5 Bepaal welke toezichthoudende autoriteit bevoegd is in het geval van internationale activiteiten. Controleer ook of derde landen voldoende bescherming bieden.

- Geen documenten

6 Zet een (voorlopige) privacy- en cookieverklaring op jouw site of pas die aan. Pas alle relevante documenten aan indien nodig.

- Privacyverklaring
- Cookieverklaring
- Informatieverklaring voor documenten zoals vacatures, e-mails en nieuwsbrieven

7 Pas de contracten met leveranciers en klanten aan (incl. verwerkersovereenkomst)

- Verwerkersovereenkomst
- Standaardbepaling met betrekking tot gegevensbescherming voor overeenkomsten

8 Stel een intern gegevensbeleid op

- Intern gegevensbeleid
- Privacyverklaring ten aanzien van werknemers
- Informatieveiligheidsbeleid
- Aanpassingen aan arbeids-/diensten-overeenkomsten en arbeidsreglement
- Opleidingsmaterialen

9 Bereid je voor op datalekken en stel een datalek-procedure op

- Register van datalekken
- Datalek-procedure
- Modelmededelingen aan betrokkenen

10 Evalueer risicovolle verwerkingsactiviteiten dmv een GEB

- Sjabloon GEB

Kenniscentrum
Data & Maatschappij