Europese Commissie

Zeven stappen voor bedrijven

om zich voor te bereiden op de algemene verordening gegevensbescherming

Justitie en Consumentenzaken

Voor wie?

Deze leidraad is bedoeld voor bedrijven waarvoor de verwerking van persoonsgegevens geen kernactiviteit vormt, zoals mkb-bedrijven die vooral te maken hebben met de persoonsgegevens van hun werknemers of bestanden hebben van klanten. Dit kunnen bijvoorbeeld handelaren of winkels zijn, zoals een bakker of slager, of dienstverleners zoals architecten. Deze leidraad geeft aan welke stappen u moet ondernemen om u voor te bereiden op de AVG.

Onder persoonsgegevens wordt alle informatie verstaan die betrekking heeft op een levende persoon (dus niet op rechtspersonen). Bijvoorbeeld: naam, achternaam, privéadres, e-mailadres of locatiegegevens van de kaart op een mobiele telefoon. Doorgaans gaat het hierbij om de gegevens die u heeft over uw werknemers, uw klanten of uw leveranciers.

Hoe minder risico's voor persoonsgegevens uw activiteiten met zich meebrengen, hoe minder u hoeft te doen

Pas deze belangrijke beginselen toe:

- **verzamel persoonsgegevens voor duidelijk omschreven doeleinden, en gebruik deze niet voor iets anders** (als u uw klanten om een e-mailadres vraagt zodat zij uw nieuwe aanbiedingen en acties kunnen ontvangen, mag u dit niet voor andere doeleinden gebruiken of doorverkopen aan een ander bedrijf).
- **verzamel niet meer gegevens dan u nodig heeft** (als u thuisbezorgt, heeft u bv. een adres en een naam bij de bel nodig, maar u hoeft niet te weten of deze persoon getrouwd is of single); ga gewoon bewust om met de persoonsgegevens die u beheert.

STAP 1 — CONTROLEER DE PERSOONSGEGEVENS DIE U VERZAMELT EN VERWERKT, DE DOELEINDEN WAARVOOR DIT GEBEURT EN OP WELKE JURIDISCHE BASIS

U heeft **werknemers**; u verwerkt hun persoonsgegevens op basis van de arbeidsovereenkomst en op basis van wettelijke verplichtingen (bv. berichtgeving aan de belastingdienst/sociale-zekerheidsinstanties).

U mag een bestand bijhouden van **individuele klanten**, bijvoorbeeld om hen te informeren over speciale aanbiedingen/advertenties als uw klanten u hiervoor toestemming hebben gegeven.

U heeft niet altijd toestemming nodig. Er zijn gevallen waarin personen ervan uitgaan dat hun gegevens worden verwerkt. Als pizzaverkoper kunt u bijvoorbeeld het bezorgadres gebruiken om een van uw nieuwe producten te promoten. Dit heet een gerechtvaardigd belang. U moet personen informeren over het beoogde gebruik en de verwerking van dergelijke gegevens staken, als zij u hierom vragen.

Als u een bestand bijhoudt van **leveranciers** of **zakelijke klanten**, dan doet u dit op basis van de contracten die u met hen heeft. Dit zijn niet noodzakelijk schriftelijke contracten.

STAP 2 — INFORMEER KLANTEN, WERKNEMERS EN ANDERE PERSONEN ALS U HUN PERSOONSGEGEVENS VERZAMELT

Personen moeten weten dat u hun persoonsgegevens verwerkt en voor welke doeleinden.

Maar u hoeft personen niet te informeren als zij al op de hoogte zijn van hoe u de gegevens gebruikt, bijvoorbeeld als een klant u vraagt om een bestelling thuis te bezorgen.

U moet personen op verzoek ook informeren over de persoonsgegevens die u over hen heeft en inzage in hun gegevens geven. Zorg ervoor dat u uw gegevens op orde houdt, zodat als bv. een werknemer u vraagt wat voor soort persoonsgegevens u heeft, u deze gemakkelijk kunt verstrekken zonder extra gedoe.

STAP 3 — BEWAAR DE PERSOONSGEGEVENS NIET LANGER DAN NODIG IS

Gegevens over uw werknemers: zo lang als de werkrelatie en bijbehorende wettelijke verplichtingen duren.

Gegevens over uw klanten: zo lang als de klantrelatie en bijbehorende wettelijke verplichtingen (bijvoorbeeld voor belastingdoeleinden) duren.

Verwijder gegevens als ze niet meer nodig zijn voor het doel waarvoor u ze heeft verzameld.

STAP 4 — BEVEILIG DE PERSOONSGEGEVENS DIE U VERZAMELT

Als u deze gegevens in een **IT-systeem** opslaat, beperk dan de toegang tot de bestanden met de gegevens, bv. door middel van een wachtwoord. Update regelmatig de beveiligingsinstellingen van uw systeem.

(Opmerking: de AVG schrijft geen specifiek IT-systeem voor)

Als u fysieke documenten met persoonsgegevens opslaat, zorg er dan voor dat onbevoegde personen hier geen toegang toe hebben; bewaar deze in een afgesloten safe of kast.

STAP 5 — HOU DOCUMENTATIE BIJ OVER UW GEGEVENSVERWERKINGSACTIVITEITEN

Stel een beknopt document op waarin u uitlegt welke persoonsgegevens u heeft en voor welke doeleinden. Het kan zijn dat u deze documentatie beschikbaar moet stellen aan uw nationale gegevensbeschermingsautoriteit, als deze hierom verzoekt.

Degelijke documenten dienen de volgende informatie te bevatten:

INFORMATIE	VOORBEELDEN
Het doel van de gegevensverwerking	Klanten attenderen op speciale aanbiedingen/thuisbezorgen; leveranciers betalen; salarissen en sociale premies voor werknemers
Het type persoonsgegevens	Contactgegevens van klanten; contactgegevens van leveranciers; gegevens van werknemers
De categorieën van personen waarop de gegevens betrekking hebben	Werknemers; klanten; leveranciers
De categorieën ontvangers	Arbeidsinstanties; belastingdienst
De bewaartermijnen	Persoonsgegevens van werknemers tot het einde van de arbeidsovereenkomst (en de bijbehorende wettelijke verplichtingen); persoonsgegevens van klanten tot het einde van de klant-/contractuele relatie
De technische en organisatorische beveiligingsmaatregelen ter bescherming van de persoonsgegevens	Regelmatige updates van uw IT-systemen; afgesloten safe/kast
Of persoonsgegevens worden doorgegeven aan ontvangers buiten de EU	Gebruik van een verwerker buiten de EU (bv. voor opslag in de cloud)

STAP 6 — ZORG ERVOOR DAT UW ONDERAANNEMERS DE REGELS RESPECTEREN

Als u de verwerking van persoonsgegevens uitbesteedt aan een ander bedrijf, maak dan alleen gebruik van een dienstverlener die verwerking conform de eisen van de AVG garandeert (bijvoorbeeld i.v.m. beveiligingsmaatregelen). Controleer voordat u een contract tekent of zij al wijzigingen hebben doorgevoerd en voldoen aan de AVG. Neem dit op in het contract.

STAP 7 — CONTROLEER OF DE ONDERSTAANDE BEPALINGEN VOOR U VAN TOEPASSING ZIJN

> Om persoonsgegevens beter te beschermen, dient u als organisatie mogelijk een verantwoordelijke voor gegevensbescherming (data protection officer – DPO) aan te stellen. **U hoeft dit echter niet te doen** als de verwerking van persoonsgegevens niet een kernactiviteit van uw onderneming vormt, de verwerking geen risico's met zich meebrengt en het niet om een grootschalige activiteit gaat.

Als uw bedrijf bijvoorbeeld alleen gegevens over klanten verzamelt voor thuisbezorging, dan hoeft u geen DPO aan te stellen.

Ook als u wel gebruik moet maken van een DPO, kan dit een bestaande werknemer zijn die deze functie vervult naast zijn/haar andere taken. Of het kan een externe consultant zijn, net zoals veel organisaties gebruikmaken van een accountant.

> **Normaal gesproken hoeft u geen effectbeoordeling voor de privacy uit te voeren**

Een dergelijke effectbeoordeling moet alleen worden uitgevoerd door degenen die een groter risico vormen voor persoonsgegevens, bijvoorbeeld bedrijven die zich bezighouden met grootschalige bewaking van publiek toegankelijke ruimten (zoals videobewaking).

Als u een klein bedrijf heeft dat salarissen van werknemers en een klantenbestand beheert, dan hoeft u geen effectbeoordeling uit te voeren.

Geldboetes

De gegevensbeschermingsautoriteiten kunnen bij inbreuk op de gegevensbeschermingsregels sancties opleggen. Zij kunnen corrigerende maatregelen nemen (zoals een berisping of een tijdelijke verwerkingsbeperking) en/of een geldboete opleggen.

De beslissing om een geldboete op te leggen moet evenredig zijn en worden gebaseerd op een beoordeling van alle omstandigheden van het betreffende geval.

Als zij besluiten een boete op te leggen, hangt het bedrag van de boete ook af van de omstandigheden per geval, waaronder de ernst van de inbreuk en de opzettelijke of nalatige aard ervan. Er wordt ook rekening gehouden met uw instelling en bedoelingen.

Indien u meer informatie wilt:

1. Bekijk de online adviezen van de Europese Commissie over de hervorming van gegevensbescherming (beschikbaar in alle EU-talen):

europa.eu/dataprotection/nl

2. Neem contact op met uw nationale gegevensbeschermingsautoriteit:

edpb.europa.eu/about-edpb/board/members_nl

BELANGRIJKE MEDEDELING

De informatie in deze leidraad is uitsluitend bedoeld om meer inzicht in de EU-regels voor gegevensbescherming te geven.

De leidraad is zuiver bedoeld als een advies. Alleen de tekst van de algemene verordening gegevensbescherming (AVG) is rechtsgeldig. Daardoor kunnen natuurlijke personen hun rechten en verplichtingen alleen ontlenen aan de AVG. Met deze adviezen worden geen afdwingbare rechten of verwachtingen gecreëerd.

Bindende interpretatie van EU-wetgeving is de exclusieve bevoegdheid van het Hof van Justitie. De in deze adviezen tot uitdrukking gebrachte opvattingen kunnen geen afbreuk doen aan het standpunt dat de Commissie mogelijk inneemt bij het Hof van Justitie.

Noch de Europese Commissie noch enig persoon handelend namens de Commissie is verantwoordelijk voor het gebruik dat van de informatie in deze leidraad zou kunnen worden gemaakt.

Omdat deze adviezen een weerspiegeling zijn van de stand van zaken op het moment dat ze werden opgesteld, moeten zij gezien worden als een „dynamisch document” dat openstaat voor verbetering. De inhoud van deze adviezen kan zonder aankondiging vooraf worden gewijzigd.

Publicatiebureau

Luxemburg: Bureau voor publicaties van de Europese Unie, 2018

Print	PDF
ISBN 978-92-79-85399-9	ISBN 978-92-79-85408-8
doi:10.2838/91652	doi:10.2838/246683
DS-02-18-544-NL-C	DS-02-18-544-NL-N