[Bedrijf] - Beleid inzake gegevensbescherming (leidraad)

[***Opmerking: dit is een intern beleid inzake gegevensbescherming dat uiteenzet hoe uw bedrijf persoonsgegevens verwerkt en richtlijnen biedt aan uw personeel over hoe persoonsgegevens moeten worden behandeld tijdens de uitvoering van hun taken***]

# Kader en doel van deze leidraad

In het kader van uw werk voor [Bedrijf] is het mogelijk dat u verschillende soorten gegevens moet opslaan, gebruiken, wijzigen of verzenden.

Als deze gegevens (direct of indirect) betrekking hebben op een natuurlijke persoon die geïdentificeerd of identificeerbaar is, zullen deze gegevens in het kader van de wetgeving van de Europese Unie inzake gegevensbescherming worden beschouwd als **persoonsgegevens**.

## Wat zijn persoonsgegevens?

‘Persoonsgegevens’ is een zeer ruim begrip. Het dekt de namen van natuurlijke personen, contactgegevens, financiële gegevens, tewerkstellingsgeschiedenis, gebruikersnamen, wachtwoorden, IP-adressen, koopgewoonten enz. Gegevens kunnen ‘persoonlijk’ blijven, zelfs als er geen naam in de betreffende databank staat. Een lijst van klantenaankopen met een ID-nummer van een klant zonder bijbehorende naam bevat nog steeds persoonsgegevens als u (of iemand anders binnen [Bedrijf], of zelfs daarbuiten) de klant-ID kan koppelen aan de naam van de natuurlijke persoon. Ook als u de leeftijd, de functie binnen een bedrijf en het telefoonnummer van een persoon kent, kent u verschillende kenmerken die u in combinatie met elkaar in staat stellen de natuurlijke persoon te identificeren.

Gegevens betreffende bedrijven kunnen ook persoonsgegevens zijn: bijvoorbeeld het e-mailadres, professioneel telefoonnummer en werkadres van een vertegenwoordiger zijn persoonsgegevens.

## Waarom deze leidraad?

Persoonsgegevens zijn een beschermde vorm van gegevens in verschillende landen en rechtsgebieden, met name de Europese Unie (EU). Als gevolg daarvan zijn er in de EU en elders regels over wat u met persoonsgegevens mag doen. Wij spreken van ‘verwerking’ van persoonsgegevens als een manier om elk (potentieel) gebruik van persoonsgegevens te dekken: het opslaan, gebruiken, wijzigen, verwijderen, verzenden, zelfs het louter geven van toegang tot of het hebben van inzage in de gegevens in kwestie (bv. toegang op afstand). Met andere woorden, **alles wat u doet met persoonsgegevens is gereglementeerd**.

We zijn daarom verplicht een strategie voor gegevensbescherming te hanteren die in overeenstemming is met de wet en die de rechten garandeert van alle mensen van wie u de persoonsgegevens verwerkt. Niet-naleving kan aanleiding geven tot aanzienlijke boetes. Daarom willen wij er als organisatie voor zorgen dat alle medewerkers die betrokken zijn bij de verwerking van persoonsgegevens op de hoogte zijn van de do's en don'ts met betrekking tot persoonsgegevens.

## Hoe verhoudt dit zich tot mijn werk?

De kans is groot dat u, ongeacht uw rol en functie, persoonsgegevens verwerkt in het kader van uw dagelijkse taken. [***GEEF VOORBEELD VOOR AFDELING/TAAK - bv. voor HR:*** Een HR-manager zal bijvoorbeeld voortdurend toegang hebben tot persoonsgegevens van werknemers en deze wijzigen; op dezelfde manier zal een verkoopvertegenwoordiger regelmatig de contactgegevens van onze klanten bijwerken of nieuwe klanten aan onze databanken toevoegen.]

In deze leidraad lichten we verschillende richtlijnen toe over wat u wel en niet mag doen met persoonsgegevens. Controleer op basis van uw taken welke aanbevelingen het relevantst zijn, maar houd altijd rekening met de andere richtlijnen in dit document.

# Do’s en don’ts inzake persoonsgegevens

Binnen [Bedrijf] moeten we ervoor zorgen dat we een op privacy gerichte cultuur hebben die ons in staat stelt onze diensten te verlenen op een manier die in overeenstemming is met de wettelijke vereisten.

Door de volgende do’s en don’ts toe te passen, zullen uw individuele acties ons helpen om deze doelstelling te bereiken.

## Algemeen

* **DO:** Pas alle beleidslijnen en documentatie van [Bedrijf] toe die betrekking hebben op uw werk.

*[Zijn er specifieke beleidsregels van toepassing binnen het Bedrijf?]*

* **DO:** Maak anderen bewust van de aanpak van [Bedrijf] inzake gegevensbescherming door te verwijzen naar de passende beleidslijnen of documentatie.

*Nieuwe klanten en leveranciers kunnen bewust worden gemaakt van de externe beleidslijnen; nieuw personeel van de interne beleidslijnen.*

* **DO:** Controleer de juistheid en het al dan niet actueel zijn van de persoonsgegevens die u verwerkt.

*Ga er nooit van uit dat de persoonsgegevens actueel zijn. Als u op de hoogte bent van een wijziging met betrekking tot persoonsgegevens over uzelf als werknemer, of over een klant of leverancier, dient u de relevante databank(en) bij te werken (of een update aan te vragen).*

*[In welke omstandigheden zou u normaal gesproken op de hoogte worden gebracht van wijzigingen in de gegevens? (bv. rechtstreeks geïnformeerd door de betrokkene, wijziging vastgelegd in een andere databank,...) Welke procedures kunt u hebben ingevoerd om gegevens te actualiseren?]*

* **DO:** Gebruik persoonsgegevens alleen voor de toegestane en voorziene doeleinden.

*Binnen [Bedrijf] verzamelen we persoonsgegevens alleen voor specifieke doeleinden. Dit omvat hoofdzakelijk [Geef een overzicht van de belangrijkste doeleinden van de verwerking van persoonsgegevens binnen het Bedrijf, zoals geïdentificeerd in het gegevensregister] De verwerking van de gegevens is dan alleen toegestaan voor die doeleinden (en verenigbare doeleinden). Het is belangrijk om ervoor te zorgen dat u binnen de grenzen van deze toegestane doeleinden blijft. Voor nieuwe initiatieven of voor verwerkingen die mogelijk verder gaan, zie paragraaf 2.6 hieronder.*

* **DO:** Beperk uzelf tot het verzamelen en verwerken van alleen de persoonsgegevens die u nodig hebt.

*Wees u ervan bewust dat [Bedrijf] het door haar verzamelen en verwerken van alle persoonsgegevens moet kunnen verantwoorden en dat het principe van de minimale gegevensverwerking vereist dat [Bedrijf] dit moet beperken tot wat noodzakelijk is. Breng de soorten persoonsgegevens in kaart die u daadwerkelijk nodig hebt en vraag alleen deze op (intern en extern).*

* **DO:** Indien u vragen ontvangt met betrekking tot gegevensbescherming, deel deze dan onmiddellijk met de [Compliance Officer] ([e-mailadres]) tenzij anderszins aangegeven.

*[Bedrijf] beschikt over procedures en documentatie om de meest voorkomende vragen te beantwoorden, en beschikt zowel intern als extern over deskundige kennis via haar adviseurs. Deel alle vragen met de [Compliance Officer] van [Bedrijf] behalve als er al een specifieke procedure is die u een antwoord geeft dat u aan de natuurlijke persoon in kwestie kunt verstrekken.*

*[Zijn er bepaalde soorten vragen die u al hebt ontvangen? Zo ja, geef voorbeelden.]*

* **DON’T:** Deel geen persoonsgegevens, zelfs niet met collega’s, behalve voor zover nodig.

*Behandel alle persoonsgegevens vertrouwelijk en beveilig ze. Geef geen toegang tot persoonsgegevens tenzij u weet dat dit noodzakelijk is, en zorg ervoor dat persoonsgegevens niet verder worden verspreid. Beperk de soorten persoonsgegevens die worden gedeeld. [Denk aan een relevant voorbeeld - bv. voor mailingcampagnes heeft uw leverancier mogelijk alleen het e-mailadres en de naam van uw klanten nodig, maar niet hun postadres. Selecteer de velden die u wilt exporteren uit uw databank of kolommen in uw Excel-bestand, doe geen volledige export van de databank.]*

## Bijzondere soorten persoonsgegevens

* **DO:** Controleer de relevante procedures of neem contact op met de [Compliance Officer] van [Bedrijf] als u ertoe wordt gebracht om persoonsgegevens te verwerken van kinderen of de gezondheid, het ras, de religieuze overtuiging of het criminele verleden (inclusief verdenkingen) van een natuurlijke persoon.

*Sommige categorieën van persoonsgegevens krijgen extra beschermingsniveaus en moeten met extra zorg worden behandeld.*

*[Mag worden verwijderd als er geen gevoelige gegevens zullen worden verwerkt door de afdeling. Besteed in het bijzonder aandacht aan persoonsgegevens inzake crimineel verleden.]*

## Uw apparatuur

* **DO:** [INDIEN VAN TOEPASSING Pas het beveiligingsbeleid van [Bedrijf] toe, inclusief het privacybeleid inzake informatiebeveiliging]. Met betrekking tot uw apparatuur moeten in het bijzonder de volgende maatregelen worden getroffen:
* **DO:** Houd uw wachtwoorden geheim en deel ze met niemand.

*Iedereen kan dat geheime briefje op uw bureau vinden. Beperk de toegang tot de gegevens van anderen.*

* **DO:** Vergrendel uw apparatuur (computer/telefoon/...) wanneer u deze niet gebruikt, om de gegevens van [Bedrijf] te beschermen.

*Als u uw apparaat niet vergrendelt, kan iemand anders uw persoonsgegevens bekijken, maar ook die van anderen waartoe hij/zij mogelijk geen toegang heeft gekregen.*

*[Zijn er systematische tekortkomingen inzake beveiliging binnen de afdeling? Gebruik deze als voorbeeld.]*

## Contactpersonen bij leveranciers/dienstverleners

* **DO:** Deel persoonsgegevens die u van leveranciers (intern en extern) hebt ontvangen alleen nadat u hebt gecontroleerd of u daartoe gerechtigd bent.

*[Denk aan voorbeelden die veelzeggend zijn - bijvoorbeeld:] Bv. indien u gebruikmaakt van een derde partij om uw gegevens te verrijken (adreswijzigingen, bijkomende informatiecategorieën,...), dan zal [Bedrijf] de betrokkene nog steeds op de hoogte moeten brengen van het feit dat zij bijkomende soorten persoonsgegevens verwerkt en erop kan vertrouwen dat de leverancier deze informatie verstrekt indien zij over bewijzen beschikt dat de volledige informatie (zie lijst in de wetgeving inzake gegevensbescherming) is verstrekt.*

## Marketing

* **DO:** Verzeker u ervan dat u het recht hebt om digitale commerciële communicatie te verzenden naar de geselecteerde ontvangers, inclusief toestemming waar nodig.

*Onder de verwante regels is toestemming vereist voor de verzending van bv. nieuwsbrieven of marketingcampagnes aan natuurlijke personen (professionelen of consumenten) per elektronische post (e-mail, sms, direct bericht op sociale media enz.), behalve wat betreft de promotie bij bestaande klanten van producten/diensten die vergelijkbaar zijn met die waarvoor zij reeds klant zijn.*

*[Verwijder als er geen marketingactiviteiten worden verricht door de betrokken afdeling.]*

## Nieuwe initiatieven, producten of diensten

* **DO:** Controleer of de beoogde verwerking al gedekt is door bestaande doeleinden en informatie.

*Zo niet, kan er verdere actie nodig zijn (informatie aan de betrokkene, documentatie over de doeleinden enz.). Lees de beleidslijnen van [Bedrijf] en neem hierover contact op met de Compliance Officer.*

*[Link naar een kopie van het register van verwerkingsactiviteiten]*

* **DO:** Controleer of u een (volledige) Gegevensbeschermingseffectbeoordeling (DPIA) dient uit te voeren.

*Zie onze DPIA-tool - met deze tool kunt u controleren of een volledige DPIA vereist is of dat u slechts beperkte informatie hoeft te verstrekken met betrekking tot uw project.*

* **DO:** Als het een website of toepassing betreft, zorg er dan voor dat de verwerking van persoonsgegevens is afgedekt door de [externe privacyverklaring] van het [Bedrijf].

*De verwerking van persoonsgegevens in nieuwe websites of toepassingen is mogelijk al afgedekt door de beschrijving in de privacyverklaring. Als dit het geval is, zijn geen specifieke maatregelen vereist (behalve het plaatsen van een link naar de privacyverklaring op de website of in de toepassing). In het andere geval moet de verklaring mogelijk worden aangepast.*

*Opmerking: er gelden specifieke regels voor het aanmaken van cookies en andere lokale bestanden op het apparaat van de gebruiker. Controleer in dit verband het cookiebeleid van [Bedrijf]. [INDIEN VAN TOEPASSING]*