# De GDPR in 10 stappen

Stap 9- DPO en DPIA

# De GDPR in 10 Stappen

# Stap 9 – DPO en DPIA

## Inleiding

Deze termen zullen u misschien niet direct bekend in de oren klinken. DPO is de Engelse afkorting voor 'functionaris voor gegevensbescherming'. DPIA is de Engelse afkorting voor 'gegevensbeschermingseffectbeoordeling'. Twee al even moeilijke woorden, reden te meer om ze in een afzonderlijke stap wat beter te duiden.

## Functionaris voor gegevensbescherming (DPO)

Een functionaris voor gegevensbescherming is iemand die als onafhankelijke partij mee waakt over uw privacybeleid.

De GDPR bepaalt dat u zo'n functionaris moet aanstellen wanneer u :

- Hoofdzakelijk belast bent met verwerkingen die vanwege hun aard, omvang en/of doeleinden een regelmatige en stelselmatige observatie op grote schaal vereist van de betrokkenen;
- Hoofdzakelijk belast bent met grootschalige verwerking van bijzondere categorieën van persoonsgegevens ( zie de definitie in stap 2) en van strafrechtelijke gegevens.

Wie aan monitoring doet van medewerkers en voertuigen op basis van systemen als 'track & trace', zal onder de eerste categorie vallen, en dus in principe een DPO moeten aanstellen, indien dat op grote schaal gebeurt.

De Gegevensbeschermingsautoriteit heeft op haar website een heel duidelijke uitleg van de voorwaarden waar een DPO aan moet voldoen, wat zijn taken zijn, …:
https://www.gegevensbeschermingsautoriteit.be/themadossier-functionaris-voor-gegevensbescherming

## Gegevensbeschermingseffectbeoordeling ( DPIA)

De GDPR bepaalt dat u voordat u een verwerking start, een beoordeling moet uitvoeren van het effect van die verwerking op de rechten en vrijheden van de betrokkenen. Maar dat moet alleen wanneer de verwerking een hoog risico inhoudt voor die rechten en vrijheden. Dit kan bijvoorbeeld het geval zijn bij:

- ✓ Het toekennen van een evaluatie of een score ( inclusief profiling en voorspelling), in het bijzonder wanneer ze gebaseerd zijn op persoonlijke aspecten van de betrokkene zoals zijn werkprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, gedrag, loyaliteit, of verplaatsingen;
- ✓ Geautomatiseerde besluitvorming met een juridisch of vergelijkbaar gevolg ( bijvoorbeeld: automatische verwerking van gegevens die beslissen om iemand wel of niet als klant, leverancier, … toe te laten)
- ✓ Stelselmatige monitoring van natuurlijke personen ( bijvoorbeeld op publiek toegankelijke ruimten)
- ✓ De niet -occasionele verwerking van gevoelige gegevens of de verwerking van gegevens van zeer persoonlijke aard
- ✓ Gegevens die op grote schaal worden verwerkt
- ✓ Matching of samenvoeging van datasets
- ✓ Gegevens over kwetsbare personen ( kinderen, geesteszieken, bejaarden, …)

- ✓ Het gebruik van nieuwe technologieën ( of nieuwe toepassingen van bestaande technologieën), waarvan de impact op de risico's voor persoonsgegevens nog niet is onderzocht.
- ✓ Verwerking van gegevens die de toegang tot een bepaalde dienst kan verhinderen (bijvoorbeeld een bank die haar klanten screent op grond van kredietinformatie om te bepalen of ze al dan niet een lening toekent.

Als vuistregel geldt dat u best een beoordeling opstelt van zodra 2 van deze 9 criteria vervuld zijn.

*Toepassing – effectbeoordeling bij "track and trace" – verplichting tot het verrichten van een effectbeoordeling*

Als er toepassingen worden gebruikt die leiden tot een stelselmatige monitoring van bepaalde werknemers of voertuigen ( zoals track & trace) en dat bovendien op een grote schaal gebeurt, zal u inderdaad op voorhand zo'n effectbeoordeling moeten uitvoeren. In onze sector zal dat dus meer wél dan niet voorvallen.

De bedoeling van zo'n beoordeling is vooraf na te gaan wat de impact ervan is of kan zijn op de rechten van de betrokkenen. Daarbij kan gebruik worden gemaakt van al bestaande studies, mits deze voldoende worden geconcretiseerd naar de situatie in België.

Zo'n beoordeling bevat ten minste:

- ✓ Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder in voorkomend geval de gerechtvaardigde belangen die u inroept;
- ✓ Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- ✓ Een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen;
- ✓ De beoogde maatregelen om de risico's aan te pakken.

Wanneer uit deze beoordeling zou blijken dat de verwerking inderdaad een hoog risico zou opleveren indien u geen maatregelen neemt om het risico te beperken, moet u voorafgaand aan de verwerking de Gegevensbeschermingsautoriteit raadplegen.

# Checklist

- ❑ Ik weet wat een DPO en een DPIA is, en wanneer ik daar (geen) gebruik van moet maken.
- ❑ Ik heb in mijn Verwerkingsregister omschreven waarom ik er desgevallend geen gebruik van moet maken.