|  |
| --- |
| **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.

**A priori zal deze verplichting niet van toepassing zijn voor de cijferberoepen.** Dat betekent echter niet dat het verboden is zo’n functionaris aan te stellen. Maar dan moet die wel voldoen aan alle voorwaarden die de GDPR oplegt ( onafhankelijkheid, …).

In dit geval dient de aanstelling van de functionaris ook gemeld te worden aan de gegevensbeschermingsautoriteit via de juiste formulier:

<https://www.gegevensbeschermingsautoriteit.be/formulier-mededeling-contactgegevens-functionaris-voor-gegevensbescherming>

Het is in elk geval nuttig dat u in uw kantoor of netwerk één persoon aanduidt om deze materie (GDPR) op te volgen en die persoon zal dan ook het contactpunt zijn voor bv vragen van betrokkenen en indien nodig, de Gegevensbeschermingsautoriteit ( bv. bij een datalek).

### 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.

Indien u een DPIA wilt uitvoeren kunt u de tool opgemaakt door de CNIL (Franse autoriteit voor de gegevensbescherming) testen op volgende link: <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>. Dit is beschikbaar in verschillende talen.

A priori zal deze verplichting **niet van toepassing** zijn voor de cijferberoepen.

**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.**
 |