|  |
| --- |
| **Le RGPD en 10 étapes**Etape 9- DPO et DPIA  |

## **Le GDPR en 10 étapes**

## **Etape 9 – DPO et DPIA**

### Introduction

Ces termes vous sont peut-être inconnus. DPO est l’abréviation anglaise désignant le ‘délégué à la protection des données’. DPIA est l’abréviation anglaise désignant l’‘analyse d’impact relative à la protection des données’. Deux notions tout aussi complexes, raison de plus pour mieux les décrypter dans une étape séparée.

### Le délégué à la protection des données (DPO)

Un délégué à la protection des données est une personne qui, en qualité de partie indépendante, veille sur votre politique de protection de la vie privée.

Selon le RGPD, vous devez désigner un tel délégué lorsque vous :

* êtes chargé à titre principal de traitements qui, de par leur nature, l’étendue et/ ou les finalités, exigent une observation régulière et systématique à grande échelle des personnes concernées;
* êtes chargé à titre principal d’un traitement à grande échelle de catégories particulières de données personnelles (voir la définition à l’étape 2) et de données pénales.

**A priori, cette obligation ne sera pas d’application aux professions économiques.** Cela ne signifie toutefois pas qu’il soit interdit de désigner un tel délégué à la protection des données. Mais en cas de désignation, il sera obligatoire de remplir toutes les obligations imposées par le RGPD (indépendance,...).

Dans ce cas, la désignation du délégué, doit en outre être communiquée à l’Autorité de la protection des données via le formulaire adéquat : <https://www.autoriteprotectiondonnees.be/formulaire-de-communication-des-coordonnees-du-delegue-a-la-protection-des-donnees>

Il est en tout cas indiqué de désigner dans votre cabinet ou au sein de votre réseau une personne chargée de suivre les aspects GDPR et qui agira en tant que personne de contact pour les personnes concernées et l’APD (par exemple en cas de fuite de données).

### Analyse d’impact relative à la protection des données ( DPIA)

Selon le RGPD, avant de débuter le traitement de données, vous devez réaliser une analyse de l’impact de ce traitement sur les droits et libertés de la personne concernée. Mais cette analyse ne devra avoir lieu que lorsque le traitement comporte un risque élevé pour les droits et libertés. Cela peut se produire dans les cas suivants:

* L’octroi d’une évaluation ou d’un scoring ( en ce compris le profilage et les prévisions), en particulier lorsqu’il (elle) se base sur des aspects personnels de la personne concernée comme ses prestations de travail, sa situation économique, sa santé, ses préférences personnelles, son comportement, sa loyauté ou ses déplacements;
* Une décision automatique pouvant entraîner des effets juridiques ou similaires (par exemple le traitement automatique des données qui a pour conséquence l’acceptation ou non de quelqu’un en tant que client, fournisseur...);
* La surveillance systématique des personnes physiques (par exemple l’accès à des espaces ouverts au public);
* Le traitement non occasionnel de données sensibles ou le traitement de données de nature très personnelle
* Les données qui sont traitées à grande échelle;
* Le croisement ou le regroupement de données;
* Les données concernant des personnes vulnérables (enfants, malades mentaux, personnes âgées, …);
* L’usage de nouvelles technologies (ou les nouvelles applications de technologies existantes), dont l’impact sur les risques pour les données personnelles n’a pas encore été examiné.
* Le traitement de données qui peut empêcher l’accès à un service déterminé (par exemple une banque qui filtre ses clients sur la base d’informations de crédit pour déterminer si elle accorde ou non un crédit).

Retenons comme principe de base qu’il vaut mieux réaliser une analyse d’impact à partir du moment où 2 de ces 9 critères sont remplis.

Si vous voulez réaliser une analyse d’impact, vous pouvez suivre le modèle réalisé par la CNIL (régulateur des données personnelles en France), accessible sur le site suivant : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>. Ce modèle peut être utilisé en plusieurs langues.

**A priori, cette obligation ne sera pas d’application aux professions économiques.**

**Checklist**

|  |
| --- |
| * **Je sais ce qu’est un DPO et un DPIA, et lorsque je n’ai pas l’obligation d’en faire usage.**
* **J’ai défini dans mon Registre de traitement des activités la raison pour laquelle je ne dois pas en faire usage le cas échéant.**
 |