

Profil de poste : Le Délégué à la protection des données

Rédigé Par:

**Sébastien CLAUDE**

Délégué à la protection des données

***Date de publication: 05/09/2018***

|  |  |  |
| --- | --- | --- |
| **Historique** | | |
| Version | Date de modification | Champ des modifications |
| 1,0 | 22/04/2018 | Création |
| 1,1 | 23/08/2018 | Changement de charte graphique |

|  |  |  |  |
| --- | --- | --- | --- |
| **Légitimité** | | | |
| **Rédigé par :**  Mr S. CLAUDE,  DPD GHT  Le | **Validé par :**  Le : | **Vérifié par :**  Mr S. CLAUDE,  DPD GHT  Le : | **Approuvé par :**  Le : |

Sommaire

[I. Introduction 3](#_Toc523930100)

[1 ) Contexte : Qu’est ce que le RGPD 3](#_Toc523930101)

[2 ) le DPO obligatoire ! Mais pour Qui ? 3](#_Toc523930102)

[II. Les missions du DPD 5](#_Toc523930103)

[III. Les compétences requises 5](#_Toc523930104)

[IV. Les connaissance nécessaires au DPD 6](#_Toc523930105)

[V. Ses responsabilités 7](#_Toc523930106)

[VI. Quelle protection pour le délégué à la protection des données ? 8](#_Toc523930107)

# Introduction

## Contexte : Qu’est ce que le RGPD

L’acronyme RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l’Union européenne.

Le contexte juridique s’adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s’inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l’utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l’Union Européenne en se fondant sur la confiance des utilisateurs.

Il n’existe pas d’exceptions à ces obligations pour les entreprises et organisations françaises. Toutefois, selon leur activité, elles seront plus ou moins concernées par cette législation. En effet, l’approche du RGPD est fondée sur la notion de gestion de risques, offrant ainsi des marges de manœuvre pour définir des solutions sur mesure.

Ces nouvelles obligations incitent notamment à plus de transparence dans les relations avec les interlocuteurs : clients, salariés, prospects, fournisseurs, etc.

Une meilleure connaissance de l’usage qui sera fait de leurs données et des conditions d’exercice de leurs droits renforcera la confiance et favorisera donc l’activité, y compris à l’export.

## le DPO obligatoire ! Mais pour Qui ?

La désignation d’un délégué est obligatoire pour :

* Les autorités ou les organismes publics,
* Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
* Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors des cas de désignation obligatoire, la désignation d’un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l’identification et la coordination des actions à mener en matière de protection des données personnelles.

Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé c’est-à-dire désigné pour plusieurs organismes sous certaines conditions. Par exemple, lorsqu’un délégué est désigné pour un groupe d’entreprises, il doit être facilement joignable à partir de chaque lieu d’établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l’autorité de contrôle.

# Les missions du DPD

Le délégué à la protection des données a été défini par le règlement général de protection des données comme le coordinateur au sein d’une entreprise qui doit assurer les missions suivantes :

* **contrôler** le respect du règlement et du droit national en matière de protection des données ;
* **informer** et **conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
* **conseiller** l’organisme sur la réalisation d’une **analyse d'impact** relative à la protection des données et d’en vérifier l’exécution ;
* **coopérer** avec l’autorité de contrôle et d’être le point de contact de celle-ci (voir question ci-après). En France il s’agit de la **CNIL**

Les missions du DPD couvrent l’**ensemble des traitements** mis en œuvre par l’organisme qui l’a désigné.

Le délégué **n’est pas personnellement responsable** en cas de non-conformité de son organisme avec le règlement.

En tant que point de contact pour l’autorité de protection des données, le délégué doit faciliter l’accès par l’autorité aux documents et informations dans le cadre de l’exercice des missions et des pouvoirs de cette autorité (par exemple lors d’échanges avec l’autorité dans l’instruction d’une plainte, ou en cas besoin de précisions sur un projet en cours ou bien encore, dans le cadre d’un contrôle de l’autorité).

L’obligation de confidentialité ou de secret professionnel du délégué ne doit pas l’empêcher de demander conseil à l’autorité sur tout sujet, si nécessaire.

# Les compétences requises

Le délégué doit être désigné « sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions » (article 37.5 du règlement européen).

La personne qui a vocation à devenir délégué à la protection doit pouvoir réunir les qualités et compétences suivantes :

* l’**aptitude à communiquer** efficacement et à exercer ses fonctions et missions en toute indépendance. Le délégué ne doit **pas avoir de conflit d’intérêts avec ses autres missions**. Cela signifie qu’il ne peut occuper des fonctions, au sein de l’organisme, qui le conduise à déterminer les finalités et les moyens d’un traitement (éviter d’être « juge et partie »)
* une **expertise en matière de législations** et **pratiques en matière de protection des données**, acquise notamment grâce à une formation continue. Le niveau d’expertise doit être adapté à l’activité de l’organisme et à la sensibilité des traitements mis en œuvre.
* une bonne **connaissance du secteur d’activité et de l’organisation de l’organisme** et en particulier des opérations de traitement, des systèmes d’information et des besoins de l’organisme en matière de protection et de sécurité des données.
* un **positionnement efficace** en interne pour être en capacité de **faire directement rapport au niveau le plus élevé** de l’organisme et également d’**animer un réseau** de relais au sein des filiales d’un groupe par exemple et/ou une équipe d’experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.).

**La rigueur, l’écoute et la communication** sont des valeurs qui peuvent faciliter les relations avec les agents et les usagers d’une structure. Il convient donc que le choix d’un candidat pour ce poste en tienne compte.

# Les connaissances nécessaires au DPD

Pour pouvoir exercer ses missions de façon la plus opérationnelle possible le DPD va devoir acquérir les connaissances suivantes si il n’en maîtrise pas déjà les fondamentaux :

* La gestion de risque : Il s’agit d’évaluer de façon pragmatique les risques encourus en cas de violation de données. Dans ce contexte une connaissance de l’ISO 27001 ou de la méthodologie EBIOS sera une aide indéniable au DPD pour la réalisation de ses missions.
* L’amélioration continue (Roue de Daeming) : le RGPD a été élaboré sur la base de ce principe il convient donc d’en connaître l’application pour que le DPD puisse s’organiser au mieux et conduire l’organisme progressivement vers une meilleure gestion et une sécurité accrus des données.
* L’urbanisation d’un système d’information : pour comprendre le fonctionnement et la mise en œuvre d’un traitement un minimum de connaissance sur ce domaine seront nécessaire à la bonne compréhension des traitements effectués.
* Des connaissances juridiques dans le pays d’exécution du traitement et ou des personnes concernées par le traitement. Il s’agit avant tout d’un texte juridique il est donc important de connaître la structure et l’applicabilité des différents outils qui vont découlé du RGPD.

# Ses responsabilités

Quelle est la responsabilité du délégué à la protection des données ?

La responsabilité du délégué est similaire à celle du CIL. Les lignes directrices du G29 précisent que **le délégué n’est pas responsable en cas de de non-respect du règlement**. Ce dernier établit clairement que c’est **le responsable du traitement (RT) ou le sous-traitant (ST)** qui est tenu de s’assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24.1 du règlement). Le respect de la protection des données relève donc de la responsabilité du RT ou du ST.

Il **n’est pas possible de transférer au Délégué**, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. En effet, cela reviendrait à conférer au Délégué un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d’un conflit d’intérêts contraire à l’article 38.6 du règlement européen.

En France, il existe des situations où le délégué pourrait comme n’importe quel autre employé ou agent, voir sa responsabilité pénale engagée. Ainsi, la responsabilité pénale d’un délégué pourrait être retenue s’il enfreint intentionnellement les dispositions pénales de la loi Informatique et Libertés ou en tant que complice s’il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions pénales.

Le DPD **est soumis au secret professionnel ou à une obligation de confidentialité** en ce qui concerne l’exercice de ses missions, conformément au droit de l’Union ou au droit des États membres,

# Quelle protection pour le délégué à la protection des données ?

Le délégué doit agir **d’une manière indépendante** et bénéficier d’une protection suffisante dans l’exercice de ses missions. Le règlement prévoit ainsi que le délégué **ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement** ou le sous-traitant pour l’exercice de ses missions.

Les sanctions ne sont pas possibles si elles sont imposées en raison de l’exercice par le délégué de sa fonction. A titre d’exemple, si un délégué estime qu’un traitement est susceptible d’engendrer un risque élevé et conseille au responsable de traitement de procéder à une analyse d’impact, et si le responsable de traitement n’est pas d’accord avec l’analyse du délégué, ce dernier ne peut être relevé de sa fonction pour avoir formulé ce conseil.

Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s’agir, par exemple, d’absence de promotion ou de retard dans la promotion, de freins à l’avancement de carrière ou du refus de l’octroi d’avantages dont bénéficient d’autres employés. Il n’est pas nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu’elle soit utilisée pour sanctionner le délégué pour des motifs liés à ses activités en tant que délégué.

A noter toutefois que **le délégué n’est pas un salarié protégé au sens du code du travail français**. Dès lors, il pourrait être licencié légitimement, comme tout autre employé, pour des motifs autres que l’exercice de ses missions de délégué (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou fautes graves similaires).