RGPD : le délégué à la protection des données (DPO)

Description

Le délégué à la protection des données ou DPO est chargé de la mise en conformité des organismes au RGPD. Il a été consacré par le Règlement Général sur la Protection des Données (RGPD) en rendant sa désignation obligatoire dans certains cas. L'objectif du RGPD est de renforcer le contrôle des individus sur leurs données s'inscrivant ainsi dans la continuité de la Loi Française Informatique et Libertés de 1978. La violation de la vie privée des personnes concernées peut donner lieu à des sanctions.

Obtenir un devis gratuit RGPD

Qu'est-ce que le délégué à la protection des données (DPO) prévu par le RGPD ?

Au sein de l'organisme privé ou public qu'il intègre, le DPO est le **responsable de la protection des données à caractère personnel**. Les données à caractère personnel sont des informations qui se rapportent à une personne vivante identifiée ou identifiable. Au quotidien, les entreprises traitent de nombreuses données à caractère personnel qui sont très sensibles. Il est donc nécessaire de désigner un professionnel qui va **se charger de la gestion responsable** de l'ensemble de ces données. Jusqu'en mai 2018, la désignation de cette personne, qui était le Correspondant Informatique et Libertés (CIL), était totalement facultative. Avec le RGPD, la nécessité d'un responsable des données personnelles s'est accrue au point où certains organismes ont l'obligation de désigner un **délégué à la protection des données personnelles**.

Attention : Les données de santé bénéficient d'une protection renforcée car elles sont hautement sensibles.

Quel est le rôle du délégué à la protection des données (DPO) selon le RGPD ?

Le DPO est chargé de **piloter la conformité au RGPD**. En effet, son rôle est de mettre en œuvre la conformité au règlement européen sur la protection des données

au sein de l'organisme l'ayant désigné. Il joue le rôle d'intermédiaire entre l'organisme et la CNIL afin de veiller au **respect de la vie privée et des libertés fondamentales** des personnes dont les données sont collectées et traitées.

Missions du délégué à la protection des données à caractère personnel

La principale mission du DPO est d'assurer la mise en conformité au RGPD de l'organisme qui l'a désigné. À cet effet, il est chargé de remplir les fonctions listées à l'article 39 du RGPD:

- Informer et conseiller l'organisme ainsi que ses employés ;
- Contrôler le respect du règlement ainsi que du droit national en matière de protection des données ;
- Jouer l'interlocuteur des personnes concernées par les questions relatives à la protection des données personnelles ;
- Coopérer avec la CNIL.

Le délégué à la protection des données doit tenir compte du risque lié à la sensibilité des données et donc s'assurer que leur collecte et leur traitement se font dans un contexte bien déterminé qui cadre avec la finalité.

Sa mission se décline en une démarche active et énergétique qu'il doit **garder sur le long terme** :

- Cartographier les traitements de données effectués par l'organisme ;
- Prioriser les actions à mener en ayant conscience des risques potentiels ;
- Gérer les risques en menant une analyse d'impact pour chacun des traitements des données à caractère personnel susceptible d'engendrer des risques élevés ;
- Organiser les procédures internes afin de prévenir les risques éventuels pouvant survenir tout au long du traitement ;
- Documenter la conformité en rassemblant et en organisant la documentation nécessaire.

Mener à bien toutes ces missions requiert le respect de principes tels que le principe d'accountability du RGPD ou le privacy by design mentionné dans le RGPD.

Le RGPD recommande la mise en place, dans le cadre des missions du délégué à la protection des données (DPO), de certains outils tels que la tenue du registre de traitement de données effectué par l'entreprise et une analyse d'impact relative à la protection des données personnelles.

Critères régissant l'exercice de la fonction

Le DPO est investi d'une fonction assez délicate. Il est le **garant des droits et libertés fondamentales** des personnes dont les données sont collectées et traitées au sein de l'organisme. Il doit s'assurer que la mise en œuvre du traitement de ces données respecte les exigences posées par le RGPD. Pour cela, ce dernier **bénéficie d'un cadre légal** lui permettant d'exercer au mieux sa fonction à travers les conditions listées à l'article 38 du RGPD :

- L'indépendance des DPO ;
- Des moyens suffisants pour l'exercice de ses fonctions.

A noter : Les fonctions et responsabilités du DPO ne doivent pas occasionner de situations de conflit d'intérêts. Il est impossible de cumuler la fonction de RH, ou encore d'avocat représentant ou conseiller, avec celle de DPO au sein du même organisme.

Quelle est l'étendue de sa responsabilité?

Le délégué à la protection des données (DPO) n'est pas responsable de la non-

conformité de l'entreprise aux exigences du RGPD. Il bénéficie également d'une totale indépendance à l'égard du personnel de l'organisme qui l'a désigné.

Principe de coresponsabilité

La responsabilité du DPO **ne peut pas être engagée** en cas de non-respect des exigences du RGPD par l'organisme. Il ne dispose pas de pouvoir décisionnel concernant la finalité et les moyens du traitement des données personnelles. C'est le **principe de co-responsabilité du responsable du traitement et des sous-traitants** qui s'applique.

Attention : Le transfert de responsabilité du responsable du traitement au DPO est interdit.

Indépendance à l'égard du personnel

Le DPO est **indépendant du reste du personnel** de l'organisme. Par conséquent, le responsable de traitement ou les sous-traitants ne peuvent pas le relever de ses fonctions.

Bon à savoir : Le DPO peut être tenu pénalement responsable s'il viole intentionnellement une quelconque disposition pénale du RGPD ou de la loi informatique et Libertés.

Quelles conditions remplir pour devenir délégué à la protection des données (DPO) conformément au RGPD ?

Un certain nombre de **compétences sont nécessaires** pour répondre efficacement aux besoins du poste de DPO. **La certification DPO**, bien que n'étant pas obligatoire, permet d'identifier le niveau des expertises du délégué à la protection des données.

Compétences nécessaires à l'exercice de la fonction

L'article 37-5 du RGPD dispose que « *Le délégué à la protection des données est 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 les missions visées à l'article 39* ».

Les qualités professionnelles recherchées chez un DPO sont principalement :

- Une bonne connaissance du cadre législatif et réglementaire en ce qui concerne les exigences posées par le RGPD ;
- Connaissance du secteur d'activité de l'organisme, notamment des opérations de traitement, des systèmes d'information, ainsi que des besoins de l'organisme ;
- La maîtrise des techniques de gestion de projet.

En outre, l'**absence de conflit d'intérêt** avec ses autres missions est obligatoire pour le délégué à la protection de données à caractère personnel lorsque cette fonction est exercée à temps partiel.

Certification DPO facultative

L'exercice de la fonction de délégué à la protection des données à caractère personnel ne nécessite pas forcément la certification. Cependant, mise en place par la CNIL, la certification DPO peut s'avérer bénéfique non seulement pour l'entreprise mais aussi et surtout pour le professionnel. Elle permet d'**instaurer un climat de confiance** avec l'organisme car elle démontre que les professionnels **répondent aux exigences de compétences et de savoir-faire** posées par le RGPD, se démarquant ainsi sur un marché de plus en plus concurrentiel. Un système de référence est proposé par la CNIL à cet effet.

Organisé par des structures de certification agréées par la CNIL, l'examen de compétence consiste en un QCM qui prend la forme d'étude de cas.

Faut-il obligatoirement désigner un DPO ?

La désignation du correspondant informatique et libertés était totalement facultative avec la Loi Informatique et Libertés de 1978. Le RGPD quant à lui, instaure une obligation de désignation d'un délégué à la protection des données (DPO) dans certains cas.

Désignation obligatoire ou facultative selon le cas

Selon l'article 37-7 du RGPD, il **existe 3 cas dans lesquels il faut procéder obligatoirement à la désignation d'un délégué** à la protection des données :

1. Autorités et organismes publics (exception faite des juridictions dans l'exercice de leurs fonctions juridictionnelles) ;

2. Organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
3. Organismes dont les activités de base les amènent à traiter à grande échelle des données sensibles.

En dehors de ces trois catégories d'organismes, la désignation d'un délégué à la protection des données à caractère personnel est facultative.

Toutefois, la CNIL encourage la désignation d'un DPO au sein des entreprises qui traitent des données à caractère personnel. L'entreprise reste soumise aux exigences du RGPD. La désignation du DPO est avantageuse pour l'entreprise afin de **prévenir et réduire le risque juridique** lié au traitement des données à caractère personnel et de mettre en place de manière concrète la conformité de l'entreprise au règlement. L'organisme d'accueil peut le charger de la rédaction de la politique de confidentialité RGPD de l'entreprise.

Mode de désignation du délégué à la protection des données

Plusieurs conditions doivent être réunies pour désigner un DPO. Ce dernier doit :

- Détenir les compétences requises ;
- Disposer de moyens suffisants ;
- Avoir la capacité d'agir en toute indépendance.

Lorsque le professionnel que l'organisme souhaite désigner en tant que DPO remplit les prérequis, la désignation s'effectue sur le site de la CNIL où il sera question d'indiquer les informations suivantes :

- Numéro SIREN de la structure ou ses coordonnées (si elle ne dispose pas d'un numéro SIREN) ;
- Informations relatives au délégué désigné ;
- Informations publiques du délégué (les moyens pour être contacté par le public).

Que devient le CIL à l'épreuve du RGPD ?

Le RGPD a modifié profondément le rôle du CIL. Autant il est possible de désigner le CIL comme DPO, autant les deux peuvent cohabiter.

Modification profonde du rôle du CIL

Avec la Loi Informatique et Libertés, la présence du correspondant informatique et libertés était facultative au sein de tout organisme. Il avait pour mission principale de veiller à la conformité de l'organisme à la Loi Informatique et Libertés. Par ailleurs, il devait également justifier d'un bon niveau de connaissances en ce qui concerne la gestion des données sensibles que sont les données à caractère personnel. Face à l'évolution des modes de vie vers une plus forte consommation des produits du numérique engendrant de nouveaux défis et de nouveaux risques de violation de la vie privée des consommateurs, le RGPD a **fait évoluer le rôle du CIL**. Il instaure le DPO presque en remplacement du CIL.

Possibilité de désigner le CIL comme DPO

Le correspondant informatique et libertés au sein d'un organisme avant l'entrée en vigueur du RGPD **peut être désigné DPO**. Il faut alors s'assurer qu'il remplisse tous les critères en termes de connaissances spécialisées et de qualités professionnelles propres au DPO. Le rôle du délégué à la protection des données personnelles (DPO) est plus vaste et plus contraignant, en ce qu'il ne s'agit pas d'un rôle de conseil ou de facilitateur du respect de la Loi Informatique et Libertés, mais plutôt d'un **rôle de garant du respect des exigences du RGPD**.

Possible cohabitation du CIL et du DPO

La réglementation en vigueur n'interdit pas d'avoir au sein d'un même organisme un correspondant informatique et libertés et un délégué à la protection des données. Le plus important est qu'ils **permettent la mise en conformité** de l'organisme aux exigences du RGPD. Ils **devront agir de concert afin d'assurer la sécurité des données sensibles**. La présence du DPO va permettre de prendre en compte la sécurité depuis la conception ou la collecte jusqu'après le traitement des données à caractère personnel.

Zoom : Le traitement des données à caractère personnel demande de plus en plus une démarche responsable afin de prévenir les risques d'atteinte à la vie privée des personnes concernées. Legalplace vous propose un devis de mise en conformité RGPD économiquement avantageux et qui vous permet un véritable gain de temps.

FAQ

Faut-il obligatoirement désigner un DPO ?

La désignation d'un délégué à la protection des données n'est obligatoire que dans 3 cas listés par l'article 37 du RGPD : Le traitement des données est effectué par une autorité publique ou un organisme public, excepté les instances judiciaires agissant dans l'exercice de leur fonction juridictionnelle ; Les organismes dont les activités de base les conduisent à la réalisation d'un suivi constant et systématique des personnes à grande ampleur ; Les organismes dont les activités de base les amènent à traiter un grand volume de données sensibles. Dans tous les autres cas, elle est facultative mais fortement conseillée par la CNIL.

Le DPO engage-t-il sa responsabilité dans l'exercice de ses fonctions ?

La fonction du délégué à la protection des données est très délicate. Afin de mener à bien ses missions, il jouit d'une totale indépendance vis-à-vis du personnel de l'organisme qui l'a désigné. Il n'est pas décideur au sein de l'organisme. A cet effet, il ne peut être responsable de la non conformité de l'organisme aux exigences du RGPD. Cette responsabilité revient au responsable du traitement.

Le délégué à la protection des données doit-il être obligatoirement interne à l'organisme ?

Le délégué à la protection des données peut être interne comme externe à l'organisme. En tant qu'externe, il peut être une personne physique comme une personne morale (cabinet d'avocats ou de conseil).