Devenir délégué à la protection des données

Le délégué à la protection des données est au cœur du nouveau règlement européen. Les lignes directrices adoptées dans leur version finale le 5 avril 2017 par le G29, groupe des « CNIL » européennes, clarifient et illustrent d'exemples concrets le nouveau cadre juridique applicable en mai 2018 dans toute l'Europe.

Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du délégué, sous peine de sanctions.

Les lignes directrices du G29 ont pour objectif d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions. Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

A retenir

Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Pour garantir l'effectivité de ses missions, le délégué :

- doit disposer de qualités professionnelles et de connaissances spécifiques,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

La désignation d'un délégué est obligatoire pour :

1. Les autorités ou les organismes publics,
2. Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. 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 lignes directrices du G29 clarifient les critères posés par le règlement, notamment les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique.

Qui peut être délégué ?

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 ») (*voir la question spécifique sur le conflit d'intérêts*).
- 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.).

Il n'existe donc **pas de profil type** du délégué qui peut être une personne issue du domaine technique, juridique ou autre. Une étude menée pour la CNIL en 2015 a en effet montré que les CIL proviennent de domaines d'expertise très variés (profil technique à 47%, profil juridique à 19% et profil administratif à 10%).

Dans quel cas peut-il exister un conflit d'intérêts ?

La fonction de délégué peut être exercée à temps plein ou à temps partiel. Dans ce dernier cas, le délégué ne peut occuper des fonctions au sein de l'organisme le conduisant à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »). L'existence d'un conflit d'intérêts est donc **appréciée au cas par cas**.

A titre d'exemple, les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts : *secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle* **si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement**.

Un conflit d'intérêt peut également exister par exemple si un délégué sur la base d'un contrat de service représente l'organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données à caractère personnel.

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 CIL (et le délégué) pourrait comme n'importe quel autre employé ou agent, voir sa **responsabilité pénale** engagée. Ainsi, la responsabilité pénale d'un CIL/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.

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).

Quelles sont les missions du délégué à la protection des données ?

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

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

Les missions du délégué couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.

Les lignes directrices détaillent le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement.

Elles indiquent que **le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement**.

Que signifie coopérer avec l'autorité de contrôle et être le point de contact avec celle-ci ?

L'une des missions du délégué est d'être le point de contact pour l'autorité de protection des données et de coopérer avec elle. A ce titre, 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.

Quels sont les moyens d'action du délégué à la protection des données ?

Le délégué doit bénéficier du soutien de l'organisme qui le désigne. L'organisme devra en particulier :

- **s'assurer de son implication** dans toutes les questions relatives à la protection des données (exemple : communication interne et externe sur sa désignation)
- **lui fournir les ressources nécessaires** à la réalisation de ses tâches (exemples : formation, temps nécessaire, ressources financières, équipe)
- **lui permettre d'agir de manière indépendante** (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions)
- **lui faciliter l'accès aux données et aux opérations de traitement** (exemple : accès facilité aux autres services de l'organisme)

- **veiller à l'absence de conflit d'intérêts.**

Les lignes directrices fournissent des exemples concrets et opérationnels des ressources nécessaires à adapter selon la taille, la structure et l'activité de l'organisme. S'agissant du conflit d'intérêts, le délégué ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (ne pas être juge et partie). L'existence d'un conflit d'intérêt est appréciée au cas par cas. Les lignes directrices indiquent les fonctions qui, en règle générale, sont susceptibles de conduire à une situation de conflit d'intérêts.

Comment organiser la fonction de délégué à la protection des données ?

En vue de la préparation à la fonction de délégué, il est recommandé de :

- s'approprier les nouvelles obligations imposées par le règlement européen, en s'appuyant notamment sur les lignes directrices du G29 (portabilité, autorité chef de file, analyse d'impact).
- confier au CIL ou au futur délégué les missions suivantes :

    - **réaliser l'inventaire des traitements** de données personnelles mis en œuvre ;
    - **évaluer ses pratiques et mettre en place des procédures** (audits, *privacy by design*, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
    - **identifier les risques** associés aux opérations de traitement ;
    - **établir une politique de protection des données personnelles** ;
    - **sensibiliser les opérationnels et la direction** sur les nouvelles obligations.