DROIT DES SOCIÉTÉS

FOCUS SUR LE DPO (DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

Le règlement UE n°2016/679 du 27 avril 2016 dit « Règlement Général sur la Protection des Données » (ci-après « RGPD ») est entré en vigueur le 25 mai 2018. La loi n°2018-493 du 20 juin 2018 a modifié les dispositions de la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés » afin de la mettre en conformité avec ces nouvelles règles européennes.

Le RGPD responsabilise les entreprises s'agissant des données à caractère personnel qu'elles collectent et traitent et ouvre de nouveaux droits aux personnes physiques. Sur ce fondement, entre le 25 mai et le 1er octobre 2018, la CNIL a dénombré 742 notifications de violations concernant les données de 33 727 384 personnes situées en France ou ailleurs. 185 de ces notifications de violations concernent le secteur de l'hôtellerie tandis que la CNIL a annoncé que cinq sociétés d'assurance ont été mises en demeure pour détournement de la finalité des données des assurés. La moitié des causes de ces violations reposent sur des actes de piratage, des logiciels malveillants ou de l'hameçonnage (« l'hameçonnage ou phishing est une forme d'escroquerie sur internet. Le fraudeur se fait passer pour un organisme que vous connaissez *(banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de « mettre à jour » ou de « confirmer vos informations suite à un incident technique », notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.)* » (définition du site internet www.cnil.fr).

Parmi les différentes mesures prévues par ledit règlement, la création du délégué à la protection des données (DPD), désigné de manière générale sous l'acronyme anglais « DPO » *(Data Protection Officer)*, déjà désigné dans près de 24 500 organismes, mérite une attention particulière. La CNIL parle d'un véritable « pilote » ou encore d'un « chef d'orchestre » chargé de veiller à la mise en œuvre du règlement concernant le traitement des données à caractère personnel. Il est possible de soutenir qu'il est le successeur du Correspondant Informatique et Libertés.

Pour mieux comprendre l'intérêt de ce nouvel acteur, il convient de s'intéresser à sa désignation (I), aux conditions à remplir pour être désigné DPO (II) et enfin à ses missions (III).

I. Obligation de désignation d'un DPO

La nomination d'un DPO n'est obligatoire que dans certains cas, à savoir :

1°/ lorsque le traitement est effectué par une autorité publique ou un organisme public ;
2°/ lorsque les activités de bases consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
3°/ lorsque les activités de base consistent en un traitement à grande échelle de données sensibles.

Néanmoins, pour les autres organismes qui ne sont pas obligés de désigner un délégué à la protection des données, il est tout de même fortement recommandé d'en nommer un. Si la structure choisit de ne pas le faire, il est conseillé de pouvoir justifier de la raison pour laquelle aucun DPO n'a été désigné. Cela s'explique simplement par le fait que les organismes devront être capables de démontrer le respect du règlement en cas de contrôle.

II. Conditions à remplir pour être désigné DPO

Puisque le délégué sera un réel référent s'agissant de la mise en œuvre et du respect du règlement au sein de l'organisme, le RGPD précise les qualités et les compétences attendues de ce dernier.

Il est énoncé que le DPO devra 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 les missions »* qui lui sont confiées. Ces dispositions ne restreignent pas cette nomination à un profil type mais au contraire elles permettent à toute personne justifiant de ces qualités et compétences de prétendre à ces fonctions, si ce n'est que le DPO ne doit pas avoir de conflit d'intérêts avec ses autres fonctions.

En outre, il est important de mentionner que la CNIL a adopté récemment deux délibérations en date du 20 septembre 2018 (n°2018-318 et n°2018-317) précisant les conditions pour obtenir la certification de délégué à la protection des données. Cette certification n'est pas obligatoire mais, encore une fois, elle permettra de justifier que les exigences de compétences et de savoir-faire du délégué à la protection des données prévues par le règlement sont respectées. Pour pouvoir accéder à la certification, le candidat doit remplir l'une des deux conditions suivantes :

1°/ justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles ;
2°/ justifier d'une expérience professionnelle d'au moins 2 ans ainsi qu'une formation d'au moins 35 heures en matière de protection des données personnelles reçues par un organisme de formation.

Il est prévu que cette certification soit délivrée par des organismes certificateurs accrédités par la CNIL sur la base d'un référentiel élaboré par cette dernière.

Ces compétences spécifiques permettront à la personne désignée en qualité de délégué à la protection des données d'assurer le rôle majeur qu'elle aura au sein de l'organisme s'agissant de la protection des données personnelles.

III. Missions du DPO

En vertu du règlement, les missions du DPO consistent à informer et conseiller l'organisme ou la structure sur qui pèse l'obligation de respecter le règlement européen. À ce titre, il pourra, en particulier, être amené à se tenir informé des nouvelles obligations, à sensibiliser les acteurs ou encore à mener diverses actions. Ainsi, il a un véritable devoir d'accompagnement mais cela va également au-delà puisque le règlement lui confie également une mission de contrôle, de même qu'il sera l'interlocuteur chargé de coopérer avec l'autorité de contrôle.

En application du règlement européen, le DPO peut exercer ses missions :

- soit sur la base d'un contrat de service pour lequel, il a, d'ailleurs, été annoncé par l'Association française des correspondants à la protection des données à caractère personnel la création d'une assurance responsabilité civile professionnelle spécifique ;
- soit en qualité de membre du personnel. Dans ce dernier cas, le délégué à la protection des données bénéficie d'un véritable statut pour mener à bien ses missions. En effet, il sera en lien étroit avec la Direction de l'organisme qui l'a désigné. Ce dernier devra, d'ailleurs, faciliter le travail du DPO en mettant notamment à sa disposition des ressources nécessaires à l'exercice de ses missions, en le rendant disponible et en lui permettant d'agir en toute indépendance sans instruction particulière et sans être pénalisé ou relevé de ses fonctions.

C'est pourquoi la désignation d'un DPO chargé de « piloter » la conformité au RGPD au sein de l'organisme et d'être l'interlocuteur privilégié concernant cette problématique constitue l'un des moyens préconisés par la CNIL pour se conformer aux nouvelles exigences inhérentes au traitement de données à caractère personnel.

Jean-Pascal CHAZAL,
Avocat spécialiste en droit commercial
Sophie WATTEL,
Avocat spécialiste en droit du travail
Clémence LARGERON,
Documentaliste

CADRA
Cabinet d'Avocats en Droit des Affaires