LA FONCTION DE DPO D'UNE SOCIÉTÉ

L'article 37 du Règlement général sur la protection des données (ci-après « RGPD ») impose aux sociétés de désigner un délégué à la protection des données (DPD en français ou, ci-après, « DPO » pour Data Protection Officier en anglais) lorsque :

- le traitement est réalisé par une autorité publique ou un organisme public, à l'exception des tribunaux ; ou
- les activités de base de la société consistent en des opérations, qui en raison de leur nature, de leur étendue ou de leurs finalités, requièrent le suivi régulier et systématique de données à une large échelle ; ou
- les activités de base de la société consistent à traiter à une large échelle des données sensibles ou relatives à des condamnations ou infractions.

Néanmoins, de nombreuses entreprises décident de désigner un DPO, bien qu'elles ne se situent dans aucun des cas de désignation obligatoire susmentionnés.

En effet, la mise en conformité d'une société avec le RGPD commence par la mise en place d'une politique générale de protection des données au sein de l'entreprise, laquelle prend du temps. Or, le DPO constitue l'une des pierres angulaires de la construction d'une telle politique.

Il est donc souvent opportun de désigner au plus tôt le DPO de la société et de communiquer ensuite sur cette nomination auprès des salariés et des personnes concernées par les traitements de la société, et ce même si cette désignation n'était pas obligatoire au sens de l'article 37 du RGPD.

La finalité première de la désignation d'un DPO est d'encourager un contrôle interne. A ce titre, le DPO a la charge d'assurer, d'une manière indépendante, le respect des obligations prévues par le RGPD.

PROFIL DU DPO

Le RGPD n'impose pas de profil et ne détermine pas de condition de forme à la désignation du DPO.

La plupart des DPO désignés dépendent de la Direction Juridique ou de la Direction des Systèmes d'Information.

Debora COHEN

L'article 37-5 du RGPD précise d'ailleurs 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 ».

La Cnil a précisé que le DPO doit détenir les compétences requises, disposer des moyens suffisants pour exercer sa mission et avoir la capacité d'agir en toute indépendance.

Une entreprise dont le candidat répond à ces prérequis peut commencer à effectuer la désignation de son DPO à l'aide du formulaire en ligne proposé sur le site internet de la Cnil.

Cette désignation comporte quatre étapes à l'occasion desquelles il convient d'identifier l'organisme désignant le DPO, identifier le DPO, communiquer les coordonnées publiques. La dernière étape est constituée du récapitulatif de la demande et de son envoi à la Cnil.

MISSIONS DU DPO

Le DPO a des missions nombreuses et variées. Il est notamment en charge de :
- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en vertu du règlement et des autres dispositions de l'Union ou de l'État membre concerné en matière de protection des données ;
- contrôler la conformité du règlement aux règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel (répartition des responsabilités, formation du personnel participant aux traitements, audits) ;
- dispenser des conseils, lorsque cela est demandé, en ce qui concerne l'analyse d'impact et vérifier l'exécution des tâches ;
- coopérer avec l'autorité de contrôle ;
- faire office de point de contact pour l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel,

et en matière de sécurité, de :
- conseiller l'organisme sur les nouvelles manières d'exploiter les données ;
- permettre d'éviter les erreurs stratégiques lors du lancement de nouveaux services ou produits et d'optimiser en conséquence les investissements ;
- mettre en place la politique d'archivage et d'externalisation ainsi que les procédures internes relatives à la sécurité de l'information.

Le DPO, sera l'atout majeur du responsable du traitement pour répondre au principe d'accountability (obligation pour le responsable du traitement de rendre des comptes, démontrer en permanence l'efficacité des mesures prises et leur effectivité).

Son rôle sera central et ses missions renforcées pour maintenir en conformité son entité. Il devra donner des directives pour mettre en place une véritable politique de respect de la vie privée.

DPO EXTERNALISÉ

Le délégué à la protection des données peut être un salarié de l'entreprise ou accomplir ses missions sur la base d'un contrat de service. Dans tous les cas il sera le DPO de la société.

Un DPO externe présente l'avantage de garantir une indépendance et une absence de conflit d'intérêts dans l'exercice des missions du DPO et peut apparaitre comme une solution stratégique en terme de gestion des coûts.

L'importance de la mise en conformité est telle que le DPO devra consacrer du temps dans le début de la relation afin de se familiariser avec les rouages de l'entreprise.

En présence d'un DPO externe, il est recommandé néanmoins de désigner en interne des interlocuteurs.

CONCLUSION

Que la désignation d'un DPO soit obligatoire ou non, il n'en demeure pas moins qu'elle comporte de nombreux avantages, compte-tenu des nombreuses obligations que le RGPD met à la charge des entreprises amenées à collecter et à réaliser des traitements de données à caractère personnel.

Le DPO, qu'il soit interne ou externe, doit mettre en œuvre une approche proactive et fournir une vision panoramique et de proximité pour s'adapter aux questions de la société et former les équipes de l'entreprise à appréhender ces notions.

Debora Cohen
Avocat en protection des données personnelles
Cabinet DC Avocat