Les éditeurs de contenus et services en ligne | GESTE

DESIGNER UN DPO

UNE NOUVELLE OBLIGATION POUR LES PROFESSIONNELS

Le règlement relatif à la protection des données personnelles (RGDP) consacre l'obligation, pour les entreprises, de désigner un délégué à la protection des données (data protection officer en anglais – DPO) : articles 37 et suivants.
L'entrée en application du règlement étant prévue au 25 mai 2018, il est d'ores et déjà essentiel de s'y préparer, notamment en désignant un DPO.

Le DPO, obligatoirement désigné dans certains cas prévus par le règlement (article 37), a pour principale mission de s'assurer de la mise en conformité de l'entreprise pour laquelle il travaille avec le RGPD.

LA DÉSIGNATION DU DPO

Selon l'article 37 du règlement européen, le recours au DPO est obligatoire dans le cas suivant, si l'organisme (responsable de traitement ou sous-traitant) :

- Appartient au secteur public
- Est amené à réaliser un suivi régulier et systématique de personnes physiques à large échelle dans le cadre de ses activités principales ;
- Traite à grande échelle des données dites "sensibles" ou relatives à des condamnations pénales et des infractions dans le cadre de ses activités principales.

En dehors de ces cas, le G29 encourage vivement les professionnels à désigner un DPO interne ou externe à l'organisme afin de confier à un expert la mise en conformité au règlement européen et, plus largement, toutes questions relatives à la protection des données personnelles ce qui permettrait notamment de limiter les risques de non-conformité. Il convient de noter que les règles rappelées ci-dessous s'appliquent que le DPO ait été désigné volontairement ou de façon obligatoire.

Le DPO ne doit pas nécessairement être un employé du responsable de traitement. Ainsi, il peut être externalisé, exécuter d'autres missions et tâches, voire être mutualisé au sein d'un groupe d'entreprises à condition de pouvoir démontrer qu'il est facilement joignable et peut se rendre disponible. En effet, le délégué doit être en mesure de communiquer facilement avec les personnes concernées et de coopérer avec l'autorité de contrôle.

En amont il est recommandé de confier au CIL ou au futur DPO les missions suivantes :

- Réaliser l'inventaire des traitements de données personnelles mis en œuvre,
- Evaluer ses pratiques et mettre en place les procédures (audits, notification des violations des données, gestion des réclamations et des plaintes, …)
- Identifier les risques liés aux traitements des données,
- Etablir une politique de protection des données personnelles,
- Sensibiliser les directions et les équipes opérationnelles sur les nouvelles obligations.

QUI DÉSIGNER ?

Le DPO doit être désigné sur la base de connaissances solides du droit et de son niveau d'expertise relatifs au droit et aux pratiques en matière de protection des données personnelles.
Le délégué doit par ailleurs disposer de qualités personnelles de dialogue et de management ainsi que de bonnes connaissances du secteur d'activité de l'organisme pour lequel il est désigné.

Les lignes directrices du G29 précisent le niveau d'expertise (qui peut varier au regard de la complexité des traitements de données et des éventuelles données sensibles traitées), les qualités professionnelles et les capacités du DPO.

LES MISSIONS DU DPO

Le DPO assurera un rôle central dans la conformité au RGPD puisque c'est à lui qu'incombe la promotion de la nouvelle culture d'entreprise portée par le RGPD dans le traitement des données personnelles. Plus précisément, comme le prévoit l'article 39 du règlement, au sein de son organisme, le DPO 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, du droit national et des règles internes à l'entreprise en matière de protection des données à caractère personnel
- 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 avec celle-ci.

Il doit faire preuve de pragmatisme et privilégier une approche en termes de risques, étant précisé que, dans l'exercice de ses missions, il est soumis au secret professionnel ou à une obligation de confidentialité.

Il est important de noter que le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le RGDP.

RÔLE DE L'ORGANISME VIS-À-VIS DU DPO

Comme le prévoit notamment l'article 38 du règlement, l'organisme joue un rôle crucial dans l'accomplissement par le DPO de ses missions. En effet, l'organisme devra :

- Soutenir le DPO
- S'assurer de son implication dans toutes les questions relatives à la protection des données en l'associant à ces questions d'une manière appropriée et en temps utiles
- Lui laisser le temps d'exercer ses missions (s'il exerce d'autres fonctions)
- Lui fournir les ressources financières, matérielles et humaines nécessaires à la réalisation de ses tâches
- Lui permettre d'agir de façon indépendante, lui faciliter l'accès aux données et aux opérations de traitement.

En effet, le délégué ne peut occuper des fonctions qui le conduisent à déterminer les finalités et les moyens des traitements.
Les coordonnées du DPO doivent enfin être publiées par l'organisme et communiquées à l'autorité de contrôle (CNIL en France).

Documentation CNIL

- Lignes directrices du G29
- Devenir délégué à la protection des données
- Règlement européen : se préparer en 6 étapes