Source : ©pe3check - stock.adobe.de

Le rôle du DPD est d'informer, de sensibiliser et de conseiller l'entreprise, de veiller au respect du RGPD, d'établir et de tenir à jour la documentation et de coopérer avec la CNIL.

Le DPD (ou DPO) : un atout pour se mettre en conformité avec le RGPD

Patrick Blandin, membre du groupe AFCROs-DM

Le RGPD a donné naissance à un nouveau métier : le Délégué à la Protection des Données (DPD) - ou Data Protection Officer (DPO) – Cette fonction est essentielle dans la mise en place, la gestion et la coordination de la protection des données en conformité avec le RGPD.

Le Règlement général sur la protection des données personnelles (RGPD - règlement 2016/679 du Parlement européen et du Conseil) est applicable et obligatoire depuis le 25 mai 2018. Son intégration dans la loi française avait été adoptée quelques jours avant. Le RGPD donne un cadre légal européen relatif aux données personnelles fondé sur un régime de responsabilité en matière de protection des données. Son objectif est de responsabiliser les acteurs et de renforcer les droits des personnes. Il s'applique à tous traitements de données personnelles, électroniques ou non.

La protection des données personnelles y est considérée comme un droit fondamental pour les personnes. Aussi, alors que le RGPD donne des droits à chaque individu (droit d'accès, à l'oubli, à la rectification, à la portabilité, etc.), il impose des devoirs et des obligations aux organismes publics ou privés : obligations de tenir des registres, d'analyse d'impact, de notifier dans les 72 heures toute violation de données personnelles, etc... Ces obligations concernent tous les organismes qui traitent des données personnelles pour leur compte ou pour le compte d'un autre organisme dans le cadre d'un service ou d'une prestation. Les données concernées sont celles de ses employés, de ses fournisseurs, de ses clients, mais également, dans le cadre plus particulier de la recherche clinique ou épidé-

miologique, celles des patients inclus dans les études.

Les actions à entreprendre sont nombreuses, entre autres :

- Modifier les procédures afin d'intégrer le RGDP dans la démarche qualité de l'organisme,
- Constituer un registre des traitements de données en précisant les objectifs, les catégories de données, les personnes y ayant accès et la durée utile de conservation de ces données,
- Faire le tri des données afin de limiter le risque et le nombre de traitements : données réellement utiles, effacement ou archivage des données...
- Respecter le droit des personnes en les informant et en leur permettant d'exercer facilement leurs droits (sous 1 mois maximum). A ce titre, dans le cadre de recherches cliniques, les notices d'information et les formulaires de consentement doivent être revus.
- Sécuriser les données : responsabilité légale de l'organisme qui les détient consistant à en maîtriser l'accès et en garantir l'intégrité.
- Réaliser une analyse d'impact pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées (données dites sensibles, à grande échelle ou transférées hors UE).
- Rajouter des clauses rappelant les obligations de chaque partie dans les contrats commerciaux, y compris pour les projets en cours, du fait que le RGPD établit désormais une responsabilité partagée entre le responsable du traitement et le sous-traitant concernant la protection des données personnelles qu'il traite en son nom.

Toutes ces actions et cette documentation ne peuvent être réalisées en toute sérénité que si elles sont orchestrées par une personne : le DPD. Cette fonction est considérée comme l'évolution naturelle du Correspondant Informatique et Libertés (CIL).

Sa désignation est obligatoire dès lors que le traitement est effectué par un organisme public, ou qu'il constitue une activité de base de l'organisme qui nécessite un suivi régulier et systématique à grande échelle, ou qu'il traite à grande échelle des données dites "sensibles". Le responsable du traitement et le sous-traitant désignent leurs DPD, publient et communiquent leurs coordonnées à la CNIL. Dans le cas où sa désignation ne serait pas obligatoire, il est toutefois fortement conseillé d'en désigner un.

Quel profil pour le DPD ?

Le rôle du DPD est d'informer, de sensibiliser et de conseiller l'organisme, de veiller au respect du règlement, d'établir et de maintenir la documentation, de pouvoir être disponible pour les personnes concernées et de coopérer avec la CNIL.

Sa fonction, nécessite non seulement un niveau d'expertise associé à des compétences techniques et juridiques, mais aussi des connaissances du secteur d'activité de l'organisme, une bonne compréhension des opérations de traitement réalisées ainsi que des qualités personnelles (intégrité, déontologie). Ces prérequis doivent être cohérents avec le niveau de risque et de protection exigée pour les données traitées. Une certification DPD peut être obtenue afin de garantir une mise en œuvre et une gestion efficace du cadre de conformité requis par la personne désignée.

Le DPD doit exercer sa fonction en toute objectivité et indépendance tout en rapportant directement à la direction. A ce titre, il ne reçoit aucune instruction venant de l'organisme et ne peut être licencié ou sanctionné pour l'exercice de ses missions. Un contrat de service peut être établi entre employeur et employé.

Désigner un DPD en interne signifie, embaucher ou dégager du temps d'une personne pour la réalisation des missions du DPD. L'organisme doit donc s'assurer que le DPD qu'il a désigné bénéficie des formations, ressources et moyens techniques nécessaires au bon exercice de ses missions, et qu'il est associé à toutes les questions relatives à la protection des données à caractères personnel dès le stade le plus précoce. Cependant, le DPD ne doit pas exercer d'autres fonctions entraînant un conflit d'intérêt avec ces missions c'est-à-dire, le conduisant à déterminer les finalités ou les moyens d'un traitement.

Un même DPD pour plusieurs entreprises

Les organismes ayant peu de moyens ou peu de compétences à dédier aux nouvelles exigences ne peuvent pas désigner leurs DPD en interne. La solution consiste alors à faire appel à un DPD externe. Comme le prévoit le RGPD, "Un groupe d'entreprises peut désigner un seul délégué à la protection des données...". Pour autant, le DPD doit être facilement joignable par les personnes concernées ou par la CNIL. Il est aussi recommandé qu'il soit localisé dans l'UE et parle dans la langue de l'organisme qui l'a désigné.

« Le DPD ne doit pas exercer d'autres fonctions entraînant un conflit d'intérêt avec ses missions. »

Patrick Blandin, membre du groupe AFCROs-DM

Des sociétés proposent des DPD sous contrat de service. L'intérêt est que les compétences peuvent être mises en commun, mais il sera alors préférable de ne désigner qu'un seul DPD comme contact principal par client. Le DPD de ce type de société de service pourra alors assumer sa fonction pour plusieurs clients.

Il est à garder en mémoire qu'à moins d'une délégation de responsabilité, la responsabilité juridique relative à la conformité au règlement reste à la charge du responsable du traitement ou du sous-traitant.

En cas de non-respect du RGPD, les sanctions sont bien loin de celles prévues par notre bonne vieille loi informatique et libertés, puisqu'elles peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires de l'organisme. *eg*

www.afcros.com

Source : AFCROs