

## LES RECOMMANDATIONS DE LA CNIL

# Le rôle clé du DPO

Un peu moins d'un an après l'entrée en application du RGPD, le régulateur rappelle, dans les colonnes de *L'Argus de l'assurance*, dans quels cas la désignation d'un délégué à la protection des données (DPO) est obligatoire et quelles sont ses prérogatives.

### LA FONCTION DE LA CNIL

La Cnil accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. Un service dédié, le service des DPO, a pour rôle de fédérer et d'animer les réseaux de DPO, de réguler l'écosystème de ce nouveau métier et de les accompagner dans leurs missions.

#### **PREMIER POINT** Quelles sont la formation et les compétences requises pour être délégué à la protection des données (DPO)?

Il n'y a pas de profil type requis pour exercer cette fonction. Ce peut être une personne issue du domaine technique, juridique ou autre. Selon le Règlement européen sur la protection des données (RGPD), celle-ci doit être désignée «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». Le DPO doit être apte à communiquer efficacement, à exercer ses missions en toute indépendance et ne pas avoir de conflit d'intérêts avec ses éventuelles autres missions. Il doit posséder une expertise en matière de législations et de pratiques de la protection des données. Une bonne connaissance du secteur d'activité et de l'organisation de l'institution est indispensable. Enfin, il doit jouir d'un positionnement efficace en interne pour être en capacité de rapporter au plus haut niveau et d'animer un réseau de relais auprès des différents services.

La Cnil vient d'adopter deux référentiels en matière de certification des compétences du DPO. Celle-ci permet aux intéressés de justifier qu'ils répondent aux exigences de compétences et de

savoir-faire prévues par le RGPD. La première étape de cette certification est l'agrément par la Cnil des organismes délivrant les certifications. Ce nouvel outil devrait être disponible en 2019.

#### **DEUXIÈME POINT** Quel est le rôle du DPO?

Il est chargé d'informer et de conseiller l'organisme qui le désigne ainsi que les 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. Enfin, il est chargé de coopérer avec l'autorité de contrôle dont il est le point de contact.

#### **TROISIÈME POINT** Dans quel type d'organisme?

La désignation d'un DPO est obligatoire pour les organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle et les organismes dont les activités de base les amènent à traiter à grande envergure des données dites «sensibles» ou relatives à des condamnations pénales et infractions. En outre, la désignation d'un DPO est fortement encouragée par le comité européen de la protection des données (CEPD, ex-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. À ce jour, 45 000 organismes ont désigné auprès de la Cnil un DPO (personnes physiques ou morales).

#### **QUATRIÈME POINT** Quelle est la responsabilité du DPO?

Les lignes directrices du comité européen de la protection des données précisent que le DPO n'est pas responsable en cas de non-respect du règlement. Cette responsabilité incombe à l'organisme. Il n'est pas possible de transférer au DPO cette responsabilité par délégation de pouvoir car cela reviendrait à conférer à ce dernier un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts contraire au RGPD.

En revanche, le délégué pourrait, comme n'importe quel autre employé ou agent, voir sa responsabilité pénale engagée s'il enfreint intentionnellement les dispositions pénales de la loi Informatique et libertés ou en tant que complice s'il aide l'organisme à enfreindre ces dispositions pénales. •