RGPD

DPO : QUELLE GOUVERNANCE POUR ÊTRE CONFORME AU RGPD ?

A la suite de l'ouverture de vingt-cinq procédures d'audit par l'Authorité de contrôle luxembourgeoise (la « CNPD »), deux enquêtes ont conduit la CNPD à condamner deux organismes qui n'avaient pas pris toutes les mesures permettant au DPO d'exercer ses missions conformément aux exigences du RGPD. Comme chaque mois, Alexandre Fiévée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en nous appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen.

« *Le délégué est chargé de piloter la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cet organisme* »[1], explique la Cnil.« *Pour garantir l'effectivité de ses missions, ajoute-t-elle, le délégué doit : disposer de qualités professionnelles et de connaissances spécifiques ; bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer efficacement ses missions* ». La désignation du DPO est obligatoire dans certains cas énumérés dans le RGPD. Dans les autres cas, sa désignation reste fortement recommandée, le DPO étant considéré comme le « *chef d'orchestre* » de la mise en conformité au RGPD de l'organisme dont il dépend. Le DPO est principalement en charge : (i) d'informer et de conseiller le responsable du traitement ou le sous-traitant, ainsi que leurs employés ; (ii) de contrôler le respect de la règlementation en matière de protection des données ; (iii) de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ; (iv) de coopérer avec l'autorité de contrôle ; (v) et d'être le point de contact des personnes concernées. Le DPO doit bénéficier du soutien de l'organisme qui l'a désigné. Ce dernier doit donc : (i) s'assurer de l'implication du DPO dans toutes les questions relatives à la protection des données ; (ii) lui fournir les ressources nécessaires à la réalisation de ses missions ; (iii) lui permettre d'agir de manière indépendante ; (iv) lui faciliter l'accès aux données et aux opérations de traitement ; (v) et veiller à l'absence de conflit d'intérêts.

Les affaires[2]

La CNPD, l'autorité de contrôle luxembourgeoise, a lancé en 2018 une campagne d'enquête thématique sur la fonction du DPD, qui s'est traduite par l'ouverture de 25 procédures d'audit concernant tant le secteur privé que le secteur public. Deux enquêtes ont été ouvertes, l'une concernant un établissement de crédit, l'autre une entreprise de transport. Plusieurs griefs ont été relevés.

Premier grief : le défaut de publication des coordonnées du DPD. « *Le DPD doit pouvoir être contacté aisément et directement via un canal de communication adapté aux personnes concernés* »[3], indique la CNPD. Or les coordonnées du DPD ne figuraient sur aucun support et n'étaient notamment pas mentionnées sur le site internet de l'organisme contrôlé.

Autre grief : le manquement à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données. Il est normal de s'attendre, selon le chef d'enquête, à ce que le DPD participe « *de manière formalisée et sur la base d'une fréquence définie, au Comité de Direction, aux comités de coordination de projet, aux comités de nouveaux produits, aux comités de sécurité ou tout autre comité jugé utile dans le cadre de la protection des données* »[4]. Le fait que la présence du DPD à ces comités ne reposait sur aucune règle ni sur une fréquence définie constitue, selon la CNPD, un manquement.

L'autorité de contrôle a constaté un autre manquement concernant l'obligation de garantir l'autonomie du DPD, celui-ci n'étant pas rattaché, dans les faits, au niveau le plus élevé de la direction comme l'impose pourtant le RGPD. « *En effet, le DPD est rattaché à une personne du département (...) qui est elle-même rattachée à une personne du département (...) qui est elle-même rattachée au Chief Compliance Officer, souligne le chef d'enquête. Bien que le DPD puisse intervenir de manière ad hoc au Comité exécutif et au Comité de contrôle interne à sa demande et à tout moment, le rattachement hiérarchique à la Direction et donc l'accès à cette dernière ne sont pas directs et permanents.* »[5]

Il était également reproché aux deux sociétés un manquement relatif à la mission de contrôle du DPD, aucun plan de contrôle n'ayant été formalisé. Selon la CNPD, « *la mission de contrôle effectuée par le DPD auprès du contrôlé devrait être suffisamment formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPD puisse effectuer sa mission de contrôle au respect du RGPD de manière adéquate* »[6].

Compte tenu de ces différents manquements, la CNPD a infligé aux deux sociétés une amende administrative d'un montant de 15.400 euros pour la première[7], et d'un montant de 18.700 euros pour la seconde[8].

Quelles recommandations ?

Depuis l'entrée en vigueur du RGPD, tout organisme doit mettre en œuvre les mécanismes et les procédures internes permettant de démontrer le respect des règles relatives à la protection des données. La fonction de DPO n'échappe pas à la règle. Le RGPD définit les compétences attendues d'un DPO et les moyens qu'il doit disposer pour exercer ses missions. Le règlement insiste par ailleurs sur la capacité du DPO d'agir en toute indépendance. A l'aune de ces deux décisions, tout organisme devrait organiser un audit de la fonction du DPO, et ce afin de vérifier que la gouvernance « *RGPD* » est conforme aux exigences règlementaires.

Alexandre FIEVEE
Avocat associé
Derriennic associés

Notes

(1) https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

(2) CNPD, délibération n° 40FR/2021 du 27 octobre 2021 ; CNPD, délibération n° 41FR/2021 du 27 octobre 2021.

(3) CNPD, délibération n° 41FR/2021 du 27 octobre 2021.

(4) CNPD, Délibération n° 40FR/2021 du 27 octobre 2021 ; CNPD, Délibération n° 41FR/2021 du 27 octobre 2021.

(5) CNPD, Délibération n° 41FR/2021 du 27 octobre 2021.

(6) CNPD, Délibération n° 40FR/2021 du 27 octobre 2021 ; CNPD, Délibération n° 41FR/2021 du 27 octobre 2021.

(7) CNPD, Délibération n° 40FR/2021 du 27 octobre 2021.

(8) CNPD, Délibération n° 41FR/2021 du 27 octobre 2021.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info