RGPD

Le DPO : dans l'œil du cyclone ? (Première partie)

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question des fonctions du DPO, et plus particulièrement celle de son positionnement dans l'organisme (Première partie). Le mois prochain, il abordera la problématique de l'exercice effectif par le DPO de ses missions (Seconde partie).

Le CEPD a annoncé, en septembre dernier, que son action coordonnée 2022/2023 portera sur les problématiques liées à la désignation du DPO et son positionnement dans les organismes. Dans le cadre de cette action coordonnée, le CEPD a invité les autorités nationales de protection des données à travailler sur le sujet.

Jusqu'à présent, l'action « *répressive* » de la Cnil sur la question du DPO, son positionnement dans l'organisme, ses ressources, ses missions a été relativement limitée. Faut-il s'attendre à ce que la Cnil diligente des missions de contrôle sur ce sujet ?

A l'aide de plusieurs décisions d'autorités de contrôle d'autres pays européens, nous allons essayer d'identifier – à partir des manquements constatés – les principales zones de risques. Ce-mois-ci nous allons aborder deux problématiques en lien avec le DPO : (i) son association à toutes les questions relatives à la protection des données dans l'organisme et (ii) son positionnement dans celui-ci vis-à-vis notamment de la direction.

En effet, il ressort des termes de l'article 38-1 du RGPD que le responsable du traitement doit veiller à ce que le délégué à la protection des données soit « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel* ». Le CEPD considère, sur cette base, que l'organisme doit s'assurer notamment (i) que le DPO participe régulièrement aux réunions de l'encadrement supérieur et intermédiaire, (ii) que sa présence est effective lorsque des décisions ayant des implications en matière de protection des données sont prises et (iii) que l'avis du DPO est dûment pris en considération. Enfin, en application de l'article 38-3 du RGPD, le délégué à la protection des données doit faire « *directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant* ».

Les affaires

Dans plusieurs décisions rendues par l'autorité de contrôle luxembourgeoise, des organismes ont été sanctionnés pour ne pas avoir correctement associé le DPO aux problématiques « *RGPD* » de l'organisme. Tel a été le cas d'une société qui ne permettait pas à son délégué à la protection des données de participer au comité directeur de manière systématique[1]. Un organisme a été également sanctionné parce que le DPO ne pouvait intervenir, que sur invitation ou de manière ad hoc, aux différentes réunions et comités dans lesquels étaient discutés les projets ayant des impacts en matière de protection des données, et ce sans qu'aucune règle ou fréquence ne soit définie[2]. Un autre cas de sanction concerne un organisme qui autorisait l'accès du DPO au comité de direction et aux réunions de gestion de projets en fonction de l'ordre du jour[3] ou encore un responsable du traitement qui n'impliquait son DPO que de manière limitée, lorsque la direction en faisait la demande expresse[4]. Enfin, il a été reproché à un organisme de n'associer qu'indirectement le DPO groupe aux questions relatives à la protection des données puisque ce dernier ne faisait pas partie du comité « *RGPD* » organisé par les filiales et n'était informé des sujets qui y étaient discutés qu'à travers les procès-verbaux. Selon l'autorité de contrôle luxembourgeoise, il y avait

là un manquement aux dispositions de l'article 38 du RGPD puisque le DPO groupe n'était finalement pas informé et surtout pas consulté « *dès le stade le plus précoce possible* » de toutes les questions relatives à la protection des données. Non seulement le DPO doit pouvoir participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire, mais il doit également pouvoir faire un rapport au niveau le plus élevé de la direction. Tel n'est pas le cas lorsqu'une telle faculté est conditionnée à l'existence et la démonstration d'un « *problème significatif* »[5], comme l'indique l'autorité luxembourgeoise de protection des données. Lorsque le délégué rend compte à une « *personne de contact* » et non directement à la direction générale, le manquement est également caractérisé, selon l'autorité belge[6]. En tout état de cause, il appartient à l'organisme de démontrer l'accès direct du DPO au plus haut niveau de direction, notamment lorsqu'il existe, dans les faits, un ou plusieurs niveaux hiérarchiques entre la direction et lui[7]. Cette démonstration est bien entendu plus aisée quand le DPO rapporte directement au comité de direction[8] ou au directeur général[9].

Quelles recommandations ?

Compte tenu de ce qui précède, il est vivement recommandé (i) d'organiser la participation directe, systématique et en temps utile du DPO aux différents comités dans lesquels sont discutées des questions portant sur la protection des données et (ii) de lui donner un accès direct et non conditionné au niveau le plus élevé de la direction. De telles actions sont indispensables pour garantir l'exercice effectif par le DPO de ses missions notamment d'information et de conseil. Bien entendu, la mise en œuvre de ces actions doit être documentée au moyen de procédures, notes internes et comptes-rendus de réunions.

Alexandre FIEVEE
Avocat Associé

DERRIENNIC ASSOCIES

Notes

(1) CNPD, Délibération n°20FR/2021, 11 juin 2021.

(2) CNPD, Délibération n°41FR/2021, 24 octobre 2021.

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

(4) CNPD, Délibération n°38FR/2021, 15 octobre 2021.

(5) CNPD, Délibération n°20FR/2021, 11 juin 2021.

(6) APD, Décision 24/2021, 19 février 2021.

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

(8) APD, Décision 56/2021, 26 avril 2021.

(9) APD, Décision 117/2021, 22 octobre 2021.