RGPD

Le DPO : dans l'œil du cyclone ?

(Seconde 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. Le mois dernier, il s'est penché sur la question des fonctions du DPO, et plus particulièrement celle de son positionnement dans l'organisme (Première partie). Ce mois-ci, il aborde la problématique de l'exercice effectif par le DPO de ses missions.

Le CEPD (Comité européen à la protection des données) a annoncé, en septembre dernier, que son action coordonnée 2022/2023 portera sur les problématiques liées à la désignation du DPO, son positionnement dans les organismes et ses missions. 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 al'organisme, ses ressources, ses missions- est restée 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 trois problématiques : la mission d'information et de conseil du DPO, ses missions de contrôle et la question de la planification de ses actions en fonction du risque.

En effet, il ressort des termes de l'article 39-1 du RGPD que le DPO a notamment pour mission d'informer et de conseiller le responsable du traitement (ou le sous-traitant) ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la règlementation ; de contrôler le respect du RGPD par l'organisme dont il dépend ; et de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et de vérifier l'exécution de celle-ci. L'article 39-2 du RGPD ajoute que le DPO tient dûment compte, dans l'accomplissement de ses missions, « *du risque associé aux opérations de traitement* » compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Les affaires

Dans plusieurs décisions rendues par les autorités luxembourgeoise (la « *CNPD* ») et hollandaise (« *l'AP* »), des organismes ont été sanctionnés pour ne pas avoir permis au DPO d'exercer ses missions d'information et de conseil. Tel a été le cas d'une société qui ne permettait pas à son délégué à la protection des données de réaliser un reporting formel et spécifique de son activité à l'encadrement supérieur, quand bien même des points réguliers étaient organisés. L'autorité luxembourgeoise a en effet considéré que, dès lors que la mission d'information et de conseil l'égard du responsable du traitement est « *intimement liée* » à l'obligation d'associer le DPO de manière appropriée et en temps utile à toutes les questions relatives à la protection des données, l'organisme avait manqué à ses obligations[1].

L'autorité hollandaise a adopté une position identique : « *Il est important que le responsable du traitement veille à ce que le DPO soit associé de manière appropriée et en temps utile à toutes les questions liées à la protection des données à caractère personnel. L'AP a établi que l'Administration fiscale et douanière n'avait pas correctement et en temps voulu associé le DPO pour mettre en œuvre une analyse d'impact (...). Il en résulte que le DPO n'a pas été en mesure d'accomplir correctement ses tâches et n'a donc pas été en mesure de conseiller à temps les autorités fiscales sur le respect du RGPD. En cas de consultation en temps opportun, le DPO aurait pu avertir plus tôt l'administration fiscale et douanière des risques associés au traitement inapproprié des données personnelles (...).* »[2]

Dans d'autres affaires, ce n'est pas le caractère effectif de la mission d'information et de conseil qui posait difficulté, mais les conditions dans lesquelles la mission de contrôle était réalisée par le DPO. Si la CNPD reconnaît que l'article 39.1 du RGPD n'impose pas à l'organisme de mette en place des mesures spécifiques pour assurer que le DPO accomplit sa mission de contrôle et que la tenue du registre des activités de traitement contribue à l'exercice de cette mission, elle relève toutefois que « *cet élément [la tenue du registre] pris isolément ne suffit pas à démontrer que la mission de contrôle du respect du RGPD est effectuée de manière adéquate* »[3].

Ainsi, selon l'autorité luxembourgeoise, « *la mission de contrôle effectuée par le DPO 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 DPO effectue sa mission de contrôle du respect du RGPD de manière adéquate.* » La CNPD a repris cette solution dans plusieurs autres affaires[4].

Enfin, dans une décision rendue par l'autorité polonaise de protection des données (« *UOPO* »), un éclairage est donné sur les attentes concernant l'article 39-2 du RGPD, selon lequel le DPO doit accomplir ses missions en tenant compte des « *risques* » liés aux opérations de traitement. Selon l'UODO : « *Cette disposition impose au délégué de fixer des priorités dans son travail, qui devrait consister à déterminer de manière individuelle et indépendante des mesures et des modalités de fonctionnement et à les adapter à la spécificité de l'organisme. Dans ce contexte, il est important d'identifier au préalable les risques liés au traitement des données personnelles et, sur cette base, de déterminer des solutions efficaces, tant techniques qu'organisationnelles. Il s'agit d'une approche sélective et pragmatique. Se concentrer sur les aspects qui comportent des risques plus élevés pour la protection des données à caractère personnel devrait permettre au DPO de conseiller plus facilement le responsable du traitement sur la méthodologie à utiliser lors de la réalisation du DPIA, sur les domaines devant être audités en interne ou en externe, sur les formations internes à planifier et réaliser pour les employés (...).* »[5]

Quelles recommandations ?

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 personnelles et donner à celui-ci un accès direct et non conditionné au niveau le plus élevé de la direction, semblent être des prérequis incontournables pour permettre au DPO d'exercer de manière effective ses missions d'information et de conseil.

Par ailleurs, il semble indispensable que l'organisme vérifie la mise en place par le DPO d'un plan d'actions comportant, parmi les actions à déployer, un plan de contrôle visant à vérifier que les préconisations qu'il a formulées ont bien été implémentées. A cet égard, il appartient au DPO de concevoir son plan d'actions selon une approche reposant sur le risque, c'est-à-dire en priorisant ses interventions et les mesures techniques et organisationnelles à mettre en œuvre en fonction des niveaux de risques identifiés.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) CNPD, Délibération n° 18FR/2021, 31 mai 2021.

(2) AP, Décision, 7 avril 2022.

(3) CNPD, Délibération n° 36FR/2021, 13 octobre 2021.

(4) CNPD, Délibération n° 38FR/2021, 15 octobre 2021 ; CNPD, Délibération n° 40FR/2021, 27 octobre 2021.

(5) UODO, Décision, 21 août 2020.

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