RGPD

Condamnation d'une banque : le DPO était « juge et partie »

La chambre de résolution des litiges de l'autorité belge de protection des données a condamné une banque pour non-respect des dispositions de l'article 38 (6) du RGPD, qui imposent à tout organisme – responsable du traitement et sous-traitant – de veiller à ce que les missions et tâches qu'exerce le collaborateur, désigné comme délégué à la protection des données (DPO), n'entraînent pas de conflit d'intérêts. 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.

Le DPO, en tant que « *chef d'orchestre* » de la conformité en matière de protection des données personnelles, peut, en application de l'article 38 (6) du RGPD, exercer, dans l'organisme dont il dépend, « *d'autres missions et tâches* ».

Il existe toutefois une limite à ce principe : il ne faut pas que ces autres missions et tâches entraînent un « *conflit d'intérêts* ».

Cette exigence, qui est étroitement liée à l'obligation pour le DPO d'agir en toute indépendance, oblige l'organisme à exclure tout collaborateur qui, dans le cadre de ses fonctions habituelles, serait amené à déterminer les finalités et moyens d'un traitement de données personnelles.

Le CEPD précise que la question du conflit d'intérêts doit être étudiée « *au cas par cas* » en considération de « *la structure organisationnelle spécifique de chaque organisme* »[1].
Il ajoute qu' « *en règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement* ».

L'affaire [2]

A l'issue d'une enquête menée par le service de l'Inspection de l'autorité belge de protection des données à l'encontre d'une banque, la Chambre de résolution des litiges a retenu contre cette dernière plusieurs manquements dont un manquement à l'article 38.6 du RGPD.

Il était reproché à cette banque un conflit d'intérêts du fait de la désignation comme DPO d'un collaborateur exerçant des fonctions de chef des départements Operational Risk Management (ORM), Information Risk Management (IRM) et Special Investigation Unit (SIU).

Selon la banque, aucun conflit d'intérêts ne pouvait lui être

opposé dans la mesure où le DPO n'avait, dans le cadre de ses autres fonctions dites de « *deuxième ligne* », que des pouvoirs purement consultatifs et de supervision.

Mais, pour la Chambre de résolution des litiges, un tel rôle ne signifie pas de facto qu'il ne détermine pas, dans le cadre de ses autres fonctions, les finalités et les moyens d'un ou plusieurs traitement(s) de données personnelles. « *L'évaluation de tout conflit d'intérêts, précise-t-elle, doit se faire au cas par cas, en tenant compte de la structure organisationnelle spécifique de chaque organisation* ».

L'élément, qui a été déterminant dans son évaluation, reposait sur le fait que, dans l'exercice de leurs pouvoirs de surveillance et de contrôle, les trois départements en question avaient besoin d'informations de la part des autres services dits de « *première ligne* », ce qui signifiait que les trois départements déterminaient la finalité et les moyens (i) « *des données à caractère personnel que le service de première ligne (devait) lui fournir* » et (ii) « *du traitement effectué par le service de première ligne afin que le service de deuxième ligne puisse remplir son rôle de contrôle et de conseil* ».

Partant, la Chambre de résolution des litiges a estimé qu'il y avait conflit d'intérêts et a sanctionné la banque pour manquement aux dispositions de l'article 38.6 du RGPD.

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.

Le choix du DPO et la délicate question du conflit d'intérêts n'échappent pas à la règle. Il pourrait ainsi être de bonne pratique pour tout organisme de recenser les fonctions qui seraient incompatibles avec celles de DPO et d'établir une règle interne visant à éviter tout conflit d'intérêts.

Il pourrait également être acté que dans une situation ponctuelle de conflit d'intérêts sur un traitement déterminé, un DPO suppléant remplace le DPO en titre dans le cadre de l'appréciation de la conformité du traitement en cause.

Alexandre FIEVEE
Avocat associé
Derriennic Associés

Notes

(1) Groupe de travail « Article 29 », Lignes directrices concernant les délégués à la protection des données (DPD), 13 décembre 2016 (version révisée et adoptée le 5 avril 2017).

(2) GBA, Décision 141/2021, 16 décembre 2021.