RGPD

Comment piloter (de manière licite) la gouvernance des données ?

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 différentes autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur le rôle et les missions du DPO dans le cadre du pilotage, conformément au RGPD, de la gouvernance des données personnelles.

Le délégué à la protection des données (« *DPD* » ou « *DPO* ») est au cœur de la conformité au règlement européen sur la protection des données personnelles (« *RGPD* »).

Ainsi, en application de l'article 39-1 du RGPD, le DPO doit notamment informer et conseiller le responsable du traitement (ou le sous-traitant) ainsi que les employés sur leurs obligations en vertu du droit applicable en matière de protection des données personnelles. Pour ce faire, l'article 38-1 du RGPD précise que le DPO doit être « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.* » Le CEPD explique que « *l'information et la consultation du DPD dès le début [doivent permettre] de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception ; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme* »[1].

Le CEPD ajoute qu'il est fondamental que le DPD soit considéré comme un « *interlocuteur* » au sein de l'organisme et qu'il soit « *membre des groupes de travail* » consacrés aux activités de traitement de données personnelles.

Afin de permettre au DPO d'exercer effectivement ses missions, l'article 38-2 du RGPD souligne que l'organisme doit l'aider « *en fournissant les ressources nécessaires* », ce qui passe, selon le CEPD, par l'octroi de « *temps suffisant* » pour qu'il puisse accomplir ses tâches, mais aussi par un « *soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant* »[2].

L'affaire[3]

Une société avait mis au point, dès 2018, une gouvernance des données en nommant un DPD au niveau du groupe et des points de contacts locaux, au niveau de chaque société. À la suite de deux contrôles (l'un sur pièces, l'autre sur place) portant sur la fonction et le rôle du DPD, l'autorité luxembourgeoise de protection des données (la « *CNPD* ») a infligé à cette société une amende administrative en raison des manquements constatés aux dispositions des articles 38 et 39 du RGPD, ainsi qu'une injonction de se conformer à ces articles 38 et 39. Cette dernière a fait appel, sans succès, de cette décision devant le Tribunal administratif du Grand-Duché de Luxembourg.

La juridiction a d'abord estimé qu'il ne ressort pas des éléments du dossier que l'intervention du DPD du groupe se faisait conformément aux exigences règlementaires, dès lors qu'il ne réalisait qu'un contrôle a posteriori des décisions d'ores-et-déjà prises par les points de contacts locaux. En d'autres termes, le DPD du groupe n'était pas associé en temps utile aux questions relatives à la protection des données personnelles. Deux éléments ont retenu l'attention de la juridiction : d'une part, le fait

qu'il n'était pas démontré la mise en place, au niveau du groupe, d'une « *politique commune* » pour les différents points de contacts locaux quant à la décision à adopter au niveau des différents traitements de données personnelles ; d'autre part, la société n'a pas été en mesure d'établir qu'il existait une « *communication régulière* » entre le DPD du groupe et ses points de contacts locaux, « *par le biais d'appels téléphoniques, de visioconférences et de courriers électroniques* », visant à échanger sur la position à adopter sur les problématiques rencontrées par ces derniers au niveau local.

La juridiction a ensuite reproché à la société de ne pas avoir quantifié ni formalisé le temps de travail que le DPD et son équipe devaient allouer à leurs missions, ni les ressources dont ils avaient effectivement besoin. En tout état de cause et sur la base des éléments en sa possession, le tribunal administratif a estimé, conformément à la décision de la CNPD, que le DPD du groupe et ses points de contact ne disposaient pas des ressources suffisantes pour exercer leurs missions : « *Force est de constater que l'activité de la demanderesse a une envergure certaine au Luxembourg pour englober (...) 70 sites, entre 1 600 et 2 100 salariés et quotidiennement 25 000 consommateurs, de sorte que, d'une part, l'exigence de la CNPD que la demanderesse aurait dû, au moins, charger une personne travaillant à plein temps sur les questions relatives à la protection des données à caractère personnel ne peut être mis en cause, et, d'autre part, que le temps de travail consacré initialement par le point de contact à ladite tâche (...), durée que la demanderesse a quantifiée comme correspondant à un travail à mi-temps, a, à juste titre, été retenue par la CNPD comme étant insuffisant.* »

Quelles recommandations ?

Dans son rapport de 2024 faisant suite aux contrôles menés par les différentes autorités nationales de protection des données dans le cadre de son action coordonnée 2023[4], le CEPD avait mis en exergue les insuffisances décrites dans l'affaire commentée. Plusieurs recommandations avaient été émises visant à encourager les organismes à se mettre dans le droit chemin... Cette décision montre qu'une organisation - qui pourtant repose sur, d'une part, un DPO groupe et, d'autre part, des points de contact locaux - reste critiquable, dès lors que le DPO ne participe pas aux prises de décisions, en laissant ses équipes – à temps partiel – participer aux réunions et ce, sans échange préalable sur la position à adopter. Il est donc fondamental, dans ce type d'organisation, que le DPO soit, grâce notamment à des ressources adaptées, davantage impliqué en amont et qu'il délivre à ses équipes des lignes directrices sur les positions à adopter selon les cas d'usage.

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) CEPD, Lignes directrices concernant le délégué à la protection des données, 5 avril 2017.

(2) CEPD, Lignes directrices concernant le délégué à la protection des données, 5 avril 2017.

(3) Tribunal administratif du Grand-Duché de Luxembourg, 4e chambre, 14 mai 2024.

(4) CEPD, rapport « Mesures d'application coordonnées - Désignation et poste des délégués à la protection des données », 16 janvier 2024.

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