RGPD

Fonctions du DPO : l'entreprise avait tout faux

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 de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question des exigences du RGPD concernant les fonctions du DPO.

La désignation d'un délégué à la protection des données (également dénommé « *Data Protection Officier* » ou « *DPO* ») est obligatoire dans les cas visés à l'article 37.1 du RGPD. Dans les autres cas, cette désignation est simplement facultative, mais largement recommandée par les autorités de contrôle et le CEPD.

Cette désignation n'est pas sans conséquence dans la mesure où elle oblige l'entreprise qui le désigne à respecter toute une série d'obligations en lien avec les fonctions du DPO (article 38 du RGPD) et ses missions (article 39 du RGPD). Ainsi, et à titre d'illustrations, l'entreprise doit : (i) 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 ; (ii) lui fournir les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, en lui permettant d'entretenir ses connaissances spécialisées ; (iii) veiller à ce qu'il ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ; (iv) s'assurer qu'il fasse directement rapport au niveau le plus élevé de la direction de l'organisation dont il relève. Enfin, l'entreprise doit garantir que, si le DPO exécute d'autres missions et tâches dans l'entreprise, celles-ci n'entraînent pas de conflit d'intérêts.

L'affaire[1]

Après avoir reçu plusieurs signalements anonymes, l'autorité norvégienne de protection des données (« *Datatilsynet* ») avait lancé une mission de contrôle à l'égard de la société mère d'un groupe d'entreprises concernant le respect, par cette dernière, des exigences relatives au délégué à la protection des données. L'inspection a révélé que la société mère agissait non seulement en tant que responsable du traitement pour certaines activités de traitement, mais aussi comme sous-traitant pour le compte des filiales et parfois comme responsable conjoint du traitement avec d'autres filiales. L'équipe en charge de la protection des données était composée du DPO de la société mère et de coordinateurs de la protection de la vie privée dans les différentes sociétés du groupe et ce, afin de garantir un lien entre le DPO et les filiales.

À, la question de savoir si le DPO était associé, de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles, Datatilsynet a répondu par la négative. D'abord parce qu'aucune procédure concernant le moment et la manière d'impliquer le DPO à toutes les questions relevant de son périmètre ne lui a été remise pendant l'inspection. Ensuite, parce que les investigations ont mis en

exergue que le DPO n'était associé aux questions « *RGPD* » qu'au cas par cas et que, lorsqu'il participait à des réunions relatives à ces questions, cela se faisait de manière informelle.

L'autorité norvégienne de protection des données s'est également intéressée au sujet des ressources allouées au DPO par l'entreprise. Constatant que le DPO occupait aussi un poste de juriste auquel il consacrait 50% de son temps, Datatilsynet a estimé que l'attribution d'un demi ETP pour la fonction dédiée à la protection des données était insuffisante. Pour en arriver à cette conclusion, l'autorité s'est notamment appuyée sur des notes internes indiquant que le DPO ne disposait pas de suffisamment de temps pour accomplir ses missions et que, la majeure partie de celui-ci, il se consacrait à « *la gestion rétroactive des problèmes, au lieu d'un travail proactif et stratégique* ».

Autre manquement constaté par Datatilsynet, le DPO ne faisait pas un rapport au plus haut niveau de direction de la société mère qui l'avait désigné. Si la description du poste mentionnait une telle exigence, l'autorité de protection des données a relevé qu'une telle formulation « *ne démontre pas l'existence d'une relation directe entre le DPO et le plus haut niveau de direction* », étant précisé que le conseil d'administration était « *officiellement* » le plus haut niveau de la société mère. Or, le DPO rendait des comptes non pas à cet organe mais au vice-président exécutif, au directeur des ressources humaines et du développement durable et au comité de conformité.

Enfin, l'autorité norvégienne de protection des données a estimé que la société mère n'avait pas procédé à toutes les évaluations qu'elle aurait dû faire concernant l'indépendance du DPO et que la distinction entre les rôles et les tâches du DPO et du juriste n'était pas suffisamment claire. « *Nous soulignons que le fait de travailler en tant que juriste n'exclut pas en soi la possibilité d'exercer les fonctions de DPO, par exemple si les conseils juridiques portent sur des domaines du droit autres que la protection des données* », a souligné l'autorité. En l'espèce, le contrôleur a relevé que le manque de clarté concernant ces deux activités était accentué par le fait que le DPO n'utilisait pas une messagerie électronique distincte selon ses activités et que sa signature électronique mentionnait ses deux rôles : « *Juriste associé et délégué à la protection des données* ». Ainsi, « *un collègue qui recevait un courriel contenant des conseils en matière de protection des données de la part du DPO était incapable de distinguer si les conseils provenaient de la fonction de DPO ou de la fonction de juriste* », en a conclu Datatilsynet.

Quelles recommandations ?

Il est fondamental de reprendre les exigences du RGPD dans la lettre de mission du DPO et dans des procédures internes, mais il convient aussi et surtout de mener une réflexion sur les conditions dans lesquelles ces exigences sont effectivement déployées dans l'entreprise. Cette réflexion doit se traduire par des notes internes et des procédures expliquant les règles en vigueur visant à garantir que les fonctions du DPO sont respectées.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) Datatilisynet, 21/03823-45, 10 mars 2025.

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