_swissprivacy.law

Économiser sur le DPO a un prix

Nathan Philémon Matantu, le 7 octobre 2024

Le DPO, même désigné pour un groupe d'entreprises, doit être associé précocement aux questions relatives à la protection des données personnelles et doit disposer des ressources nécessaires à l'exercice de ses fonctions.

Tribunal administratif du Grand-Duché de Luxembourg, jugement 46401 du 14 mai 2024

Introduction

En septembre 2018, la Commission nationale pour la protection des données luxembourgeoise (« CNPD ») procède à une enquête thématique sur la fonction de délégué à la protection des données (« *Data Protection Officer* » ou « DPO »). À cette occasion, la CPND contrôle une société luxembourgeoise active dans l'exploitation, la gestion et la fourniture de services de restauration et d'hôtellerie. Cette société emploie 2'100 personnes sur 70 sites et compte environ 25'000 clients par jour.

Lors de cette enquête, elle constate des violations des obligations d'associer le DPO à toutes les questions relatives à la protection des données à caractère personnel (art. 38 par. 1 RGPD), de lui fournir les ressources nécessaires pour exercer ses fonctions (art. 38 par. 2 RGPD) et de s'organiser de telle sorte que le DPO puisse effectivement informer et conseiller la société (art. 39 par. 1 let. a RGPD). Par décision du 31 mai 2021, la CNPD inflige à la société une amende de EUR 18'000.- et l'enjoint de se conformer aux dispositions précitées. Insatisfaite, la société sanctionnée recourt contre cette décision auprès du Tribunal administratif du Grand-Duché de Luxembourg (le « Tribunal administratif luxembourgeois »).

La participation effective du DPO, une question de timing et d'organisation

Lorsque les responsables du traitement ou les sous-traitants satisfont à l'une des conditions de l'art. 37 par. 1 RGPD, notamment lorsque les activités de traitement exigent un suivi régulier et systématique à grande échelle des personnes concernées du fait de leur nature, de leur portée et/ou de leurs finalités (art. 37 par. 1 let. b RGPD), ils doivent désigner un DPO. L'art. 37 par. 2 RGPD permet toutefois aux groupes d'entreprises de désigner un seul DPO à condition que ce dernier soit facilement joignable à partir de chaque lieu d'établissement.

Cela étant, celui-ci doit pourvoir exercer ses fonctions et remplir effectivement ses missions (art. 38 s. RGPD).

En premier lieu, le DPO doit, d'une manière appropriée et en temps utile, être associé à toutes les questions relatives à la protection des données à caractère personnel (art. 38 par. 1 RGPD). Concrétisant cette obligation, les Lignes directrices du Groupe de travail « Article 29 » concernant les délégués à la protection des données (les « Lignes directrices ») prévoient notamment que le DPO ou son équipe doit être « associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données » (chap. 3.1 p. 16). En outre, le Groupe de travail « Article 29 » (« G29 ») y ajoute que :

> « [l]'information et la consultation du [DPO] dès le début permettront 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. En outre, il importe que le [DPO] 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 au sein de l'organisme. »

En deuxième lieu, le DPO a notamment pour mission d'informer et de conseiller le responsable du traitement respectivement le sous-traitant ainsi que les employés qui traitent des données personnelles (art. 39 par. 1 let. a RGPD). Cette disposition est un corollaire de l'art. 38 par. 1 RGPD, en ce sens que le DPO ne peut exercer ses missions d'information et de conseil que s'il est associé aux questions relatives à la protection des données.

Dans le cas d'espèce, le groupe d'entreprises français auquel appartient la société luxembourgeoise dispose d'un seul DPO pour l'ensemble du groupe. Celui-ci est accompagné de deux juristes spécialisés, avec lesquels il travaille sur les questions de protection des données et définit une politique cohérente pour l'ensemble du groupe. En parallèle, chaque société du groupe dispose d'un point de contact local en charge à la fois des questions de protection des données et de la communication avec les autorités de contrôle ainsi que les personnes concernées. Des réunions entre le DPO et les points de contact locaux ont lieu au moins une fois par mois.

Au Luxembourg, le seul juriste de la société occupe le rôle de point de contact local. Au quotidien, en sus de ses tâches de juriste, celui-ci traite de toutes les questions de protection des données relatives à l'activité luxembourgeoise et rend des comptes au DPO. Avec la direc-

trice des ressources humaines, le responsable de l'audit interne, celui de l'information ainsi que l'administrateur-délégué, le point de contact siège également au sein du GDPR Board de la société luxembourgeoise. Se réunissant au moins huit fois par an, ce comité arrête la stratégie en matière de protection des données au Luxembourg, définit les plans d'action y relatifs et gère les questions opérationnelles en la matière. Le DPO ne participe pas à ces réunions, mais le point de contact local lui transmet le procès-verbal et l'informe des décisions qui y sont prises.

Le Tribunal administratif luxembourgeois analyse cette organisation et arrive à la conclusion qu'elle n'est pas conforme au RGPD. En effet, bien qu'il soit tout à fait admissible de désigner un seul DPO pour un groupe d'entreprises, l'organisation du groupe a pour conséquence que le DPO n'effectue qu'un contrôle *a posteriori* des décisions prises par le point de contact local respectivement par le GDPR Board. Faute d'association en temps utile, le DPO ne peut pas exercer ses missions d'information et de conseil. Partant, les art. 38 par. 1 et 39 par. 1 let. a RGPD sont violés.

Les ressources à disposition du DPO

L'art. 38 par. 2 RGPD impose au responsable du traitement et au sous-traitant de fournir au DPO les ressources nécessaires pour exercer effectivement ses fonctions. Dans ses Lignes directrices du Groupe Article 29 (ch. 3.2 p. 17), le G29 concrétise cette notion en énumérant les aspects à prendre en considération. En particulier, le DPO doit tout d'abord disposer de suffisamment de temps pour accomplir les missions décrites à l'art. 39 RGPD. Lorsque l'activité de DPO est exercée à temps partiel par un DPO interne ou l'est par un DPO externe, il est recommandé de fixer précisément le pourcentage alloué à l'exercice de cette activité. En outre, le DPO doit disposer de ressources financières, personnelles et techniques nécessaires. Plus les opérations sont complexes ou techniques, plus les ressources doivent être conséquentes.

En l'espèce, le Tribunal administratif luxembourgeois constate plusieurs violations de l'art. 38 par. 2 RGPD. En premier lieu, la société luxembourgeois n'a pas formellement défini le taux d'activité que le point de contact local – qui était de surcroît son seul juriste – devait réserver aux questions de protection des données.

En second lieu, l'activité de la société luxembourgeoise est importante, dans la mesure où elle emploie 2'100 personnes sur 70 sites et compte environ 25'000 clients par jour. Dans de telles circonstances, la CNPD pouvait légitimement s'attendre à ce qu'au moins une personne travaille à plein temps sur les questions relatives à la protection des données.

L'amende

Les violations de l'art. 38 par. 1 et 2 ainsi que l'art. 39 par. 1 let. a RGPD étant établies, le Tribunal administratif luxembourgeois se penche sur l'amende de EUR 18'000.- infligée par la CNPD (art. 83 par. 4 let. a RGPD). Au vu de la gravité des violations, du nombre de personnes concernées et de la durée des violations (plus de deux ans), et compte tenu de la bonne collaboration de la société luxembourgeoise, le Tribunal administratif luxembourgeois conclut que cette amende est adéquate et proportionnée.

Une appréciation

Cet arrêt met en lumière la nécessité, pour le responsable du traitement et le sous-traitant, d'assurer l'effectivité de la fonction de DPO. Ce rappel est d'autant plus important dans le contexte où le nombre de règlementations européennes en matière de nouvelles technologies accroit continuellement et que la tentation peut être grande d'attribuer d'office de nouvelles tâches au DPO (p.ex. : celles d'AI Officer). Bien qu'il soit censé de vouloir tirer profit de l'expérience du DPO en matière de nouvelles technologies, ces nouvelles attributions ne peuvent avoir lieu sans examen préalable et, le cas échéant, sans renforcement des moyens à sa disposition.

Ce rappel vaut également pour les responsables du traitement suisses, qui ont la possibilité de nommer un conseiller à la protection des données (art. 10 al. 1 LPD). En effet, celui-ci doit disposer des ressources nécessaires (art. 23 let. a OPDo) pour former et conseiller le responsable du traitement ainsi que de concourir à l'application des dispositions relatives à la protection des données (art. 10 al. 2 LPD).

Proposition de citation : Nathan Philémon MATANTU, Économiser sur le DPO a un prix, 7 octobre 2024 *in* www.swissprivacy.law/320