_swissprivacy.law

Le DPO et ses multiples casquettes face aux conflits d'intérêts

François Charlet, le 17 avril 2023

Un DPO ne peut pas se voir confier des missions ou des tâches qui le conduiraient à déterminer les finalités et les moyens d'un traitement de données personnelles. Un conflit d'intérêts ne peut être déterminé qu'au cas par cas sur la base d'une appréciation de l'ensemble des circonstances pertinentes.

Arrêt CJUE C-453/21 du 9 février 2023

Faits

Dans le cadre d'une demande préjudicielle introduite devant la Cour de justice de l'Union européenne (CJUE) par le Bundesarbeitsgericht allemand (Cour fédérale du travail), celle-ci a été invitée à interpréter l'art. 38 RGPD relatif à la fonction du délégué à la protection des données (DPO) en regard de certaines dispositions du droit allemand.

En juin 2015, l'entreprise X-FAB, sa société mère ainsi que les autres filiales de cette dernière établies en Allemagne ont désigné comme DPO le président du comité d'entreprise (c.-à-d. la représentation du personnel dans l'entreprise) de X-FAB, qui assume également la fonction de vice-président du comité central d'entreprise qui a été constitué pour trois entreprises du groupe. Cette organisation a été pensée afin d'assurer un niveau uniforme de protection des données dans lesdites entreprises.

Ces entreprises ont relevé le DPO de ses fonctions avec effet immédiat en décembre 2017, à la demande de l'autorité de protection des données du Land de Thüringen. Le 25 mai 2018, elles ont à nouveau signifié au DPO la fin de son engagement, le RGPD étant devenu applicable à cette date.

Le DPO a alors ouvert action devant les juridictions allemandes pour faire constater qu'il était toujours DPO de X-FAB, celle-ci soutenant l'existence d'un conflit d'intérêts et d'une incompatibilité avec ses deux autres fonctions (à savoir président du comité d'entreprise de X-FAB et vice-président du comité central d'entreprise). Les instances précédant le Bundesarbeitsgericht ont donné raison au DPO.

Le Bundesarbeitsgericht soumet plusieurs questions préjudicielles à la CJUE, dont celle de

savoir si les fonctions de président du comité d'entreprise et de DPO peuvent être exercées par une seule et même personne ou si cela entraîne un conflit d'intérêts incompatible avec la fonction de DPO. Cette question préjudicielle dépend de la réponse apportée à une autre question : l'art. 38 par. 3 deuxième phrase RGPD s'oppose-t-il à ce que la réglementation d'un État membre de l'UE soumette la révocation d'un DPO à des conditions plus strictes que celles prévues par le droit de l'UE ?

L'interprétation de la CJUE

La CJUE commence par rappeler que les règles prévues dans le RGPD et visant à protéger un DPO contre sa révocation ont pour seul but de préserver l'indépendance fonctionnelle du DPO. Chaque État membre est donc libre, dans la limite de ses compétences, de prévoir des dispositions plus protectrices à la condition qu'elles soient compatibles avec le droit de l'UE et le RGPD en particulier. Rappelant son arrêt C-534/20 du 22 juin 2022 dans lequel elle a jugé qu'un DPO pouvait être révoqué au motif qu'il ne posséderait plus les qualités professionnelles requises, la CJUE indique que ces dispositions plus protectrices ne doivent pas avoir pour effet de compromettre la réalisation des objectifs du RGPD (cf. www./swissprivacy.law/209/). Ainsi, l'art. 38 par. 3 deuxième phrase RGPD ne s'oppose pas *per se* à une réglementation interne plus stricte relativement à la révocation d'un DPO.

La question préjudicielle du conflit d'intérêts peut donc être analysée. Pour rappel, l'art. 38 par. 6 RGPD a la teneur suivante :

> « Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts. »

À la lecture de la première phrase de cette disposition, la CJUE déduit que « le RGPD n'établit pas d'incompatibilité de principe entre, d'une part, l'exercice des fonctions de [DPO] et, d'autre part, celui d'autres fonctions auprès du responsable du traitement ou de son sous-traitant ». Par conséquent, d'autres tâches que celles figurant à l'art. 39 RGPD peuvent être confiées au DPO à la condition qu'elles ne génèrent pas de conflit d'intérêts.. En d'autres termes, le DPO ne saurait se voir confier l'exécution de missions ou de tâches qui serait susceptible de nuire à l'exercice de ses fonctions de DPO. L'art. 38 par. 6 RGPD poursuit également le but de préservation de l'indépendance fonctionnelle du DPO.

Il en résulte qu'un DPO ne peut pas se voir confier des missions ou des tâches qui le conduiraient à déterminer les finalités et les moyens d'un traitement de données personnelles, puisqu'une de ses fonctions de DPO consiste à contrôler de manière indépendante que ces finalités et moyens respectent le droit de l'UE. Il ne peut pas être juge et partie.

La CJUE conclut que la présence d'un conflit d'intérêts ne peut être déterminée qu'au cas par cas et par le juge national, « sur la base d'une appréciation de l'ensemble des circonstances pertinentes, notamment de la structure organisationnelle du responsable du traitement ou de son sous-traitant et à la lumière de l'ensemble de la réglementation applicable, y compris des éventuelles règles internes de ces derniers ».

Commentaire général

Le raisonnement de la CJUE n'est pas surprenant pour qui connaît la teneur des Lignes directrices du Groupe de Travail Article 29 concernant les délégués à la protection des données (DPD) du 13 décembre 2016, qui indiquent que « le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas » (Lignes directrices du Groupe de Travail Article 29 concernant les délégués à la protection des données (DPD) du 13 décembre 2016, p. 28).

Tout d'abord, il convient de rappeler que la fonction de DPO peut être interne à une organisation, ou externalisée. La CJUE ne faisant aucune distinction dans son jugement, on en déduit que les règles sur le conflit d'intérêts s'appliquent également aux DPO externes.

Ensuite, la CJUE confirme (implicitement) qu'un DPO peut être démis de ses fonctions lorsque les qualités professionnelles requises pour remplir ses tâches lui font défaut.

En précisant qu'une analyse au cas par cas est nécessaire, la CJUE exige une prise en compte de tous les éléments propres à une situation particulière. L'analyse doit évidemment porter sur les éléments mentionnés dans l'arrêt, mais également sur le cahier des charges précis du DPO et des tâches qu'il mène effectivement à bien. Le conflit d'intérêts ne peut être découvert qu'après une analyse minutieuse.

D'un point de vue pratique, cet arrêt devrait inciter une organisation (et son DPO) à établir un cahier des charges très clair pour le DPO, indiquant ses tâches, prérogatives ainsi que les comportements qu'il doit éviter pour tenir éloignée la menace du conflit d'intérêts. À cette

fin, il est ainsi possible de s'inspirer des tâches et du comportement d'un auditeur, qui ne peut pas auditer son propre travail.

Dans le cas faisant l'objet du présent jugement, on ne sait pas si la fonction de président du comité d'entreprise ou celle de vice-président du comité central d'entreprise est compatible avec la fonction de DPO. On peut en douter si la représentation du personnel est amenée à traiter des données personnelles de collaborateurs dans un ou plusieurs buts que cette représentation définit (ou qui sont définies dans la loi). La réponse serait identique si elle participe, conjointement à d'autres instances de l'entreprise, à la définition des buts et moyens de certains traitements, comme ceux relatifs à la sécurité ou à la surveillance. Dans tous les cas, la représentation du personnel déciderait des moyens de chaque traitement qu'elle met en œuvre, ce qui suffirait à rendre la fonction de président de la représentation incompatible avec la fonction de DPO.

Ce jugement ne signifie pas que le DPO a l'interdiction de traiter des données personnelles. En plus de ses tâches de contrôle qui nécessiteront au moins un accès aux données, il sera souvent amené à gérer les demandes d'exercice de droit des personnes concernées. Si les finalités des traitements nécessaires à la gestion de ces demandes figurent dans la loi, les moyens à déployer pour parvenir à atteindre ces finalités sont à définir par l'entreprise, avec le concours du DPO.

Commentaire d'un DPO en exercice

Dans les faits, un DPO n'est pas toujours « que » DPO. Certaines entreprises désignent en tant que DPO leur CISO, le CFO, le responsable de la gestion des risques voire le responsable du département informatique. C'est précisément ce cumul de fonctions qui peut être problématique (et qui l'est pour les fonctions susmentionnées). Le fait que le DPO qui n'exerce pas d'autre fonction ait un cahier des charges qui prévoit des tâches qui n'ont rien à voir avec la fonction de DPO est une situation plus facile à gérer du point de vue de la prévention des conflits d'intérêts. Il n'en demeure pas moins que le DPO doit posséder les qualités professionnelles requises (notamment des connaissances spécialisées du droit et des pratiques en matière de protection des données) pour accomplir les missions que lui attribue le cadre légal (cf. art. 39 RGPD ; art. 10 nLPD). Le responsable du traitement ou le sous-traitant ne peut donc pas désigner DPO n'importe quelle personne interne ou externe à son entreprise.

La limite est parfois ténue entre les activités usuelles d'un DPO et la (participation à la) détermination des finalités et des moyens du traitement. Doit-on considérer qu'un DPO participe à la détermination de ces finalités et moyens lorsqu'il est consulté par un collaborateur qui

cherche à savoir si les actions envisagées respectent le cadre légal et que, conformément à son rôle de conseiller (art. 39 par. 1 let. a RGPD ; art. 10 al. 2 let. a nLPD), il indique au collaborateur comment procéder pour remédier à la situation ? Certains diront qu'il remplit sa fonction et que son rôle consiste précisément à orienter les collaborateurs et l'entreprise. D'autres affirmeront que la posture du DPO doit être celle d'un auditeur qui ne doit en aucun cas formuler des propositions de solutions, mais se limiter à contrôler les traitements et à signaler ceux qui ne respectent pas les dispositions légales, en rappelant la teneur de ces dernières, tout en s'abstenant de participer activement à la recherche d'une solution.

Dans de nombreuses situations, le DPO sera confronté à une demande de « validation » des mesures prises dans un projet pour respecter la législation sur la protection des données. Il est tentant de répondre positivement si tout paraît en règle, pourtant cette validation par le DPO pourrait être perçue comme une participation à la détermination des finalités ou, à tout le moins, des moyens. La différence avec la situation du paragraphe précédent réside dans la validation alors que précédemment le DPO se contentait d'offrir ses conseils. Un DPO doit ainsi prendre garde à ne jamais apposer son sceau « approuvé », tant pour des questions de conflit d'intérêts que de responsabilités civile ou pénale.

Enfin, il ne faut pas perdre de vue que le nouveau droit suisse de la protection des données diffère du droit européen sur l'exigence d'indépendance et d'absence de conflit d'intérêts du DPO. En effet, alors que le droit européen consacre cette exigence en tout état de cause (art. 38 al. 3 et 6 RGPD), le droit suisse n'impose la même chose que dans la situation où le responsable du traitement veut se soustraire à son obligation de consulter le Préposé fédéral à la protection des données et à la transparence « lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée » (art. 10 al. 3 *cum* art. 23 al. 1 et 4 nLPD). En d'autres termes, à moins que l'indépendance et l'exigence d'absence de conflit d'intérêts ne relèvent du cahier des charges du DPO, celui-ci resterait soumis aux instructions de son employeur ou de son mandant (art. 321d CO, respectivement art. 397 et 398 al. 1 CO). Le Parlement fédéral a ainsi nettement diminué le statut du DPO en droit suisse par rapport à celui que prévoit encore l'art. 12b al. 2 OLPD, ce qui est des plus regrettables.

Proposition de citation : François Charlet, Le DPO et ses multiples casquettes face aux conflits d'intérêts, 17 avril 2023 *in* www.swissprivacy.law/220

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.