Données personnelles
Fin de mission du DPO : quelles sont les règles ?

Par une décision n°406877 du 9 mars 2018, le Conseil d'Etat a estimé que la Cnil n'avait pas commis d'erreur manifeste d'appréciation en refusant de décharger de ses fonctions un correspondant informatique et libertés (CIL) pour avoir manqué à ses devoirs.

Selon le Conseil d'Etat, « *l'information des clients d'un établissement bancaire quant au risque financier qu'ils prennent en recourant à l'emprunt ne relève pas des devoirs du correspondant à la protection des données à caractère personnel de cet établissement* ». Cet arrêt, rendu avant l'entrée en application du Règlement Général de Protection des Données (RGPD), créé l'occasion d'aborder la question de la fin de mission du CIL et de sons successeur actuel : le Data Protection Officer (DPO).

En l'espèce, un particulier était en conflit avec une banque à laquelle il reprochait de ne pas l'avoir suffisamment alerté sur les risques qu'il prenait en souscrivant un prêt auprès d'elle. Il a porté plainte auprès de la Cnil et lui a demandé de destituer le CIL au motif :

- qu'il n'aurait pas respecté ses obligations et la communication de la liste complète de tous les traitements de données déclarés par la banque auprès d'elle ;
- il ressortait également des pièces du dossier que ce particulier reprochait au CIL d'avoir manqué à son devoir d'information et de mise en garde obligeant les établissements financiers à vérifier l'aptitude d'un client à rembourser un crédit consenti au regard de ses capacités financières.

Le Conseil d'Etat considère que Cnil n'a pas commis d'erreur manifeste d'appréciation en clôturant la plainte dans la mesure où dans le cadre de l'instruction de la plainte, la Cnil s'était bien assurée que la liste des traitements lui avait été communiquée. Il estime, par ailleurs, que l'information des clients d'un établissement bancaire quant au risque financier qu'ils prennent en recourant à l'emprunt ne relève pas des devoirs du correspondant à la protection des données à caractère personnel de cet établissement.

Le régime de fin de mission du CIL

Le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit divers cas de fin de mission du CIL.

Le CIL est « démissionnaire » ou « déchargé de ses fonctions »

Si le CIL est démissionnaire, il décide de sa propre initiative de mettre fin à ses fonctions de CIL tout en conservant les autres fonctions. S'il est déchargé de ses fonctions pour des raisons indépendantes de tout manquement à l'exercice de ses missions particulières, il appartient alors au responsable des traitements de notifier à la Cnil la fin de mission du CIL qui devient effectif 8 jours après.

En cas de manquements à ses devoirs, le CIL est déchargé de ses fonctions sur demande, ou après consultation de la Cnil

Une telle décharge doit être justifiée par un manquement grave, personnellement imputable au CIL et relevant directement de l'exercice de ses missions. Elle doit en outre obéir à un formalisme renforcé. Le Décret prévoit deux cas de figure :

celui où la Cnil demande au responsable des traitements de décharger son CIL de ses fonctions lorsqu'elle constate, après avoir recueilli ses observations, que celui-ci manque aux devoirs de sa mission ;
celui où c'est le responsable de traitement qui envisage de mettre fin aux fonctions de son CIL et saisit donc la Cnil pour avis.

Dans l'affaire portée devant le Conseil d'Etat le 9 mars dernier, il était donc question de la situation n°1, la Cnil n'ayant en l'occurrence pas constaté un tel manquement.

Qu'en est-il du DPO sous l'empire du RGPD ?

Un renforcement des prérogatives du DPO par rapport au CIL

Les dispositions relatives au DPO sont prévues aux articles 37, 38 et 39 du RGPD consacrés à la désignation du DPO, ses fonctions et ses missions.
La Cnil précise que le délégué à la protection des données est le successeur naturel du CIL. Leurs statuts sont similaires. Toutefois, à la différence du CIL, la désignation d'un DPO est obligatoire pour les autorités ou les organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ainsi que pour les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « *sensibles* » ou relatives à des condamnations pénales et infractions.

De plus, le RGPD pose des exigences pour la désignation du DPO en termes :

- de qualification, puisque « *Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.* » ;
- de ressources et de formation continue : le responsable de traitement ou sous-traitant doit aider le DPO à exercer ses missions « *en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.* »

Le pendant des exigences de qualification est un renforcement des missions du DPO qui devient un conseil et vecteur de sensibilisation sur les obligations du RGPD.
Nous pouvons imaginer que compte tenu du renforcement des responsabilités du DPO, celui-ci fera l'objet d'une protection renforcée. Cette protection passe par l'indépendance du DPO consacrée par le RGPD qui, en ce qui concerne ses missions, ne doit recevoir aucune instruction ou encore ne peut être relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant.

Le DPO ne rend compte qu'au niveau le plus élevé de la direction, il est soumis à une obligation de confidentialité et ne peut se retrouver en situation de conflit d'intérêt dans le cadre de l'accomplissement de tâches annexes.

Une absence de règles concernant la fin de mission du DPO

Le RGPD ne précise pas comment et quand un DPO peut être licencié ou remplacé par une autre personne. Les lignes directrices du G29 publiées le 13 décembre 2016 n'apportent pas plus d'éléments d'information sur la question. Il est toutefois précisé que le DPO, comme tout autre employé, pourra toujours être licencié légitimement pour des motifs autres que l'exercice de ses missions de DPO.
La Cnil a eu l'occasion de rappeler sur son site web que le délégué à la protection des données est le successeur naturel du CIL et que leurs statuts sont similaires. Toutefois, pour l'heure, nous sommes toujours dans l'attente de règles spécifiques applicables au DPO. Nous pouvons supposer que des règles similaires à celles du CIL seraient reprises avec, dans l'hypothèse de la destitution pour manquement grave, un renforcement des droits de la défense du DPO, avec saisine obligatoire de la Cnil, à l'image du renforcement de ses prérogatives et l'étendue de ses missions.

Les règles générales relatives au droit du travail ou au droit des contrats demeurant toutefois toujours applicables, s'agissant d'un DPO interne, la fin de sa mission pourrait être caractérisée par la fin de son contrat de travail, par exemple, une démission, un départ à la retraite, un changement de poste ou encore la non-atteinte des objectifs fixés.

S'agissant du recours à des DPO externalisés, la rupture du contrat de service dans les conditions dudit contrat de service et/ou dans les conditions du code civil, pourra constituer un motif de fin de mission. A cet égard, nous ne pouvons que recommander de bien veiller aux termes d'un tel contrat et de s'assurer des réelles compétences des organismes qui proposent ce type de mission. Les clauses importantes sont, notamment, celles relatives aux obligations du prestataire, aux modalités de résiliation en cas d'inexécution d'une obligation ou pour convenance. La cause de confidentialité apparaît également essentielle compte tenu des missions réalisées.

Par ailleurs, la Cnil soumet actuellement à consultation publique un projet de certification DPO. Une fois ce référentiel adopté, des organismes de certification agréés par la Cnil pourront délivrer des certifications de DPO sur cette base.

François-Pierre LANI
Avocat associé

Chloé KURFÜRST
Avocat
Derriennic Associés