NOTE PREPARATOIRE DE LA COMMISSION D'ACCOMPAGNEMENT POUR LA SECURITE CIVILE

DATE DE LA REUNION	Le 9 mai 2018
POINT A L'ORDRE DU JOUR	Désignation d'un data protection officer

DEMANDE A LA COMMISSION D'ACCOMPAGNEMENT	**X POUR INFORMATION** **O POUR AVIS**

THEME (L. 15.05.2007, art.16)	**O 1° le calcul des coûts supplémentaires pour les zones résultant de l'exécution de la réforme ;** **O 2° les missions qui sont confiées aux zones et leur impact financier sur la zone ;** **O 3° l'évaluation globale de tous les aspects de la réforme de la sécurité civile au niveau local. Cette évaluation contient entre autres un monitoring de tous les problèmes liés à la réforme.**

1. **<u>Problématique :</u>**

Lors de la réunion du 21 février 2018, l'UVCW a demandé des directives afin de déterminer qui peut être désigné DPO par les zones. Y a-t-il un profil spécifique ? Faut-il engager une personne externe ? Y a-t-il un risque de conflit d'intérêts avec certaines fonctions dans la zone ? 1 DPO peut-il travailler pour plusieurs zones ?

Pour votre information, vous trouverez ci-dessous une analyse, basée sur :
- le RGPD, chapitre 4, section 4 'Délégué à la protection des données';
- les Lignes directrices concernant les délégués à la protection des données (DPD) du Groupe Article 29 et
- la recommandation de la Commission de la Protection de la Vie Privée (CPVP) 04/2017 concernant la nomination d'un délégué à la protection des données et en particulier l'autorisation du cumul de cette fonction avec d'autres fonctions, dont celle de conseiller en sécurité.

Dans un souci de lisibilité, le terme 'autorité' est utilisé dans la présente note en lieu et place des termes 'sous-traitant de données' et 'responsable du traitement' [1]. Tant le sous-traitant que le responsable du traitement doivent satisfaire aux obligations du RGPD et désigner un DPO.

[1] En vertu de la loi sur la protection de la vie privée, le responsable du traitement est celui qui fixe l'objectif et les moyens du traitement des données à caractère personnel. Cependant le responsable n'est pas tenu d'assurer lui-même le traitement. Il peut désigner un sous-traitant à cet effet. C'est ainsi qu'un secrétariat social traitera par exemple les données à caractère personnel d'une entreprise ou d'une administration.

2. Solution + motivation

Le RGPD oblige toute autorité, et donc chaque zone de secours, à avoir un DPO et prévoit qu'1 DPO peut travailler pour différentes autorités (art. 37, 1, a et 3). Dans ce dernier cas, il est important que le DPO soit joignable en tout temps.

Le DPO peut être un membre du personnel interne de l'administration (dans quel cas il y a lieu d'examiner s'il cela n'entraîne pas de conflit d'intérêt entre la fonction de DPO et l'autre fonction : art 38,6) ou il peut s'agir d'une personne externe désignée via un contrat de prestation de service (art. 37,6).

L'autorité de contrôle vérifiera le respect du RGPD (et donc également des obligations en ce qui concerne le DPO). Elle vérifiera notamment si l'autorité a désigné un DPO; si le DPO peut effectivement travailler indépendant et s'il possède les qualifications requises ainsi que le temps nécessaire pour effectuer ses tâches. C'est la raison pour laquelle la CPVP recommande de documenter l'analyse et le choix final de désignation du DPO. En cas d'infraction aux obligations relatives au DPO, l'autorité de tutelle peut imposer des amendes à l'autorité.

Le DPO a au minimum pour tâche (art. 39 RGPD):

- d'accompagner l'autorité au niveau du respect des règles relatives à la protection des données (tant les règles émanant du RGPD que celles de la réglementation nationale et des règles internes) et de l'exécution des éléments essentiels du RGPD (par ex. les principes de traitement (légalité, finalité, proportionnalité), les droits des personnes dont les données sont traitées, le registre, la procédure de signalement de fuites, …) [2];
- de donner un avis à l'autorité au sujet des risques liés au traitement des données [3;]
- de fournir à l'autorité des avis relatifs aux traitements qui doivent être repris dans le registre [4;]
- de collaborer avec l'autorité de tutelle et
- d'être un point de contact sur le plan de la protection de données et ce aussi bien pour les collaborateurs, l'autorité de tutelle et les personnes dont les données sont traitées.

Lors de l'exécution de ses tâches, le DPO doit tenir compte des risques liés au traitement et de la nature, l'importance, du contexte et des finalités du traitement.

Le RGPD se limite à la description du fait que le DPO est désigné 'sur la base de ses qualités professionnelles - plus particulièrement sa connaissances spécialisée du droit et des pratiques de protection des données - et sur la base de son aptitude a effectuer ses tâches'. Il n'existe donc pas de profil légal ou d'exigence de diplôme pour le DPO.

Dans sa recommandation du 04/2017, la CPVP estime que le niveau de connaissance du DPO doit être adaptée à la sensibilité, la complexité et au volume des données traitées. Une connaissance plus étendue sera par exemple nécessaire pour le traitement de grandes quantités de données sensibles. En général, on attend du DPO qu'il dispose de connaissances professionnelles supérieures à la moyenne de la législation relative à la vie privée et de la pratique de la protection de données, et qu'il connaisse les traitements de données effectuées par l'autorité et comment est régie la sécurisation des informations. Cela implique également des connaissances du fonctionnement de l'autorité et du secteur. En fait, il doit veiller à la création d'une culture de protection des données au sein de l'organisation.

Dans sa recommandation, la CPVP n'exclut pas que le conseiller en sécurité de l'autorité assume la fonction de DPO, tout en soulignant qu'il ne s'agit certainement pas d'un automatisme. La fonction de DPO implique effectivement beaucoup plus que celle de conseiller en sécurité, qui est un informaticien et qui donne des avis sur le plan technique au sujet de la sécurisation de données, tandis que le DPO doit veiller de manière indépendante aux principes de la protection de données.

Le RGPD prévoit différentes mesures qui doivent garantir l'indépendance du DPO (art. 38):
- le DPO ne peut pas recevoir d'instructions relatives à l'exécution de ses tâches
- il rapporte directement au dirigeant le plus élevé (= le commandant ou le président de la zone)
- il a un devoir de confidentialité

[2] L'autorité (et non le DPO) est responsable de la conformité du traitement de données avec la réglementation et risque les

- il ne peut pas être licencié ou sanctionné à la suite de l'exécution de ses tâches
- il doit être notifié auprès de l'autorité de tutelle
- au sein et à l'extérieur de l'autorité, il doit être clairement identifié comme étant le DPO.
- il doit être associé en temps utile et en bonne et due forme aux questions relatives à la protection des données à caractère personnel.
- il doit disposer des moyens nécessaires à l'exécution de ses missions
- il peut combiner la fonction de DPO avec une autre fonction, mais sans entraîner un conflit d'intérêt.

Comment un conflit d'intérêt, peut-il être évité? Le DPO ne peut pas décider de son propre chef de l'objectif et des moyens du traitement des données et ne peut pas effectuer lui-même le traitement ou prendre lui-même les mesures de sécurité car, à ce moment-là, son indépendance est mise en danger.[5] Cela peut par exemple être le cas si le DPO a une fonction de management telle que CEO, chef de service ICT, finances, stratégie, marketing ou GRH, ou s'il a une autre fonction qui détermine les objectifs et les moyens du traitement.

L'autorité devra donc examiner si la fonction de DPO peut être combinée avec une autre fonction et doit identifier les fonctions incompatibles avec celles de DPO et établir des règles internes afin d'éviter tout conflit d'intérêt.

3. Conclusion

Pour résumer, le DPO doit disposer des aptitudes suivantes :
- connaissances juridiques et techniques de la protection des données,
- connaissance de l'organisation,
- connaissance du secteur et de la réglementation applicable,
- capacités humaines sur le plan de la communication et de la gestion des conflits,
- comportement éthique et intègre.

En fonction de l'importance du traitement et de la structure de l'autorité, il peut être nécessaire de constituer autour du DPO une équipe composée de différents profils ayant chacun ses propres aptitudes. La protection des données est ainsi approchée de manière holistique. La structure interne de l'équipe et les tâches et responsabilités de chaque membre devront être clairement définies.[6]

Chaque zone devra donc vérifier pour elle-même les fonctions pour lesquelles la description ci-dessus peut être un problème et devra désigner un DPO qui s'entourera, le cas échéant, de collaborateurs spécialisés sur le plan technique et/ou de la communication.

---

amendes.

[3] L'évaluation de l'impact de la protection des données comme prévu à l'art. 35 du RGPD. L'autorité doit procéder à cette évaluation, le DPO ayant uniquement une mission d'avis quant à l'exécution ou non de l'évaluation, la méthode la plus adéquate, etc. Si le DPO devait effectuer lui-même les mesures de sécurité, il ne serait plus indépendant.

[4] L'autorité est responsable de la tenue à jour du registre. Si un sous-traitant a été désigné, tant le responsable du traitement que le sous-traitent doivent tenir à jour un registre.

[5] Guidelines Group Art. 29.

[6] Recommandation 04/2017 CPVP et Guidelines Group article 29.