APDL
Association pour la Protection des Données au Luxembourg

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

CHARGÉ DE LA PROTECTION DES DONNÉES PERSONNELLES

La présente fiche a pour objectif d'apporter des précisions sur le rôle et la fonction de la personne en charge d'assurer le respect de la protection des données personnelles au sein d'une organisation : le chargé de la protection des données personnelles ou « data protection officer » (ci-après le « DPO »).

Cette fiche se base tant sur la législation luxembourgeoise en place (loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) que sur les retours d'expérience des professionnels concernés (DPO, Juristes…).

Fonction

Chargé de la Protection des Données Personnelles est une fonction définie par la loi ; en être en charge nécessite d'être au préalable **agréé** par la Commission Nationale pour la Protection des Données (« CNPD ») et **désigné** officiellement comme tel par un responsable de traitement de données à caractère personnel.

Le DPO permet au responsable du traitement d'assurer la surveillance de l'application des dispositions légales et réglementaires en matière de protection des données à caractère personnel, et ceci, au-delà même des aspects administratifs. Pour autant, le responsable du traitement conserve l'entière responsabilité des traitements de données mis en oeuvre.

Sa fonction ne doit pas être incompatible avec d'autres fonctions dont il pourrait avoir la charge, et ce, afin d'éviter des conflits d'intérêts limitant son indépendance. Par exemple, un DPO ne pourra pas occuper auprès du responsable du traitement de fonction dirigeante, être employé en tant que responsable de la sécurité des systèmes d'information et toute personne responsable de la sécurité des données en général, mais pourra très bien être Compliance Officer ou personne en charge d'identifier, évaluer et traiter les risques de non-conformité aux règles en vigueur (lois, règlements, directives, codes de conduite, standards et bonnes pratiques).

Le DPO analyse et se prononce sur tout traitement de données à caractère personnel en cours ou futur/planifié, pour s'assurer du respect de la législation en vigueur et de toutes les actions et mesures y afférentes (impact sur la vie privée des personnes concernées et niveau des mesures de sécurité nécessaires).

Une donnée à caractère personnel, c'est quoi ?

Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable. Une personne physique est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique comme par exemple un numéro de sécurité sociale, un nom, une adresse IP ou encore une adresse email.

Conditions d'exercice/organisation

Le chargé de la protection/DPO peut être interne à la société ou à l'organisme qui le désigne (salarié) ou être un prestataire externe indépendant.

Dans l'exercice de ses missions, qu'il soit interne ou externe, il est **indépendant** vis-à-vis du responsable du traitement qui le désigne ; ce dernier ne peut donc pas le limiter dans l'exercice de sa fonction ; et sauf violation de ses obligations légales ou conventionnelles, il ne peut donc pas faire l'objet de représailles de la part de l'employeur du fait de l'exercice desdites missions.

Au sein de l'entreprise/institution, il ne réfère que **directement et exclusivement à sa direction**.

Afin de pouvoir s'acquitter de ses missions, il doit disposer d'un **temps approprié et des moyens adéquats**. Par ailleurs, il doit tenir à jour ses connaissances en la matière et fournir annuellement la preuve des efforts entrepris en ce sens à la CNPD.

Les missions ou activités exercées concurremment par le DPO ne doivent **pas être susceptibles de provoquer un conflit d'intérêts** avec l'exercice de sa mission.

En cas de révocation, de démission ou d'incapacité du chargé de la protection des données, le responsable du traitement doit, s'il souhaite maintenir le recours à un chargé, procéder endéans le délai d'un mois au remplacement de ce dernier.

Conditions d'agrément

L'intéressé doit justifier d'une formation universitaire accomplie en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique ou exercer l'une des professions réglementées suivantes : avocat à la Cour, réviseur d'entreprises, expert-comptable, médecin.

La CNPD vérifie les qualités de tout chargé de la protection des données.

Missions

Le DPO peut être considéré comme le garant de l'application des dispositions légales et réglementaires en matière de protection des données à caractère personnel par le responsable du traitement qui l'a désigné. Il lui revient d'établir une gouvernance adaptée à cette fin, et pour ce faire, il doit remplir de nombreuses missions qui se recouvrent partiellement avec celles de la CNPD sans dessaisir celle-ci de ses prérogatives :

1. **Identifier** les sources potentielles de traitements de données à caractère personnel
2. **Identifier** et recenser, de façon exhaustive, les traitements impliquant des données à caractère personnel
3. **Evaluer** les risques inhérents aux traitements recensés
4. **Informer** les membres de son organisation de ces risques et des conséquences potentielles
5. **Sensibiliser** les membres de l'organisation avec le support du management et de la direction
6. **Etre** source de conseils et de recommandations
7. **S'assurer** de la prise en compte de ses conseils et recommandations lors du développement d'un nouveau traitement de données
8. **Etre** la voie de la médiation et de la coordination
9. **Tenir à jour** le registre des traitements mis en œuvre par le responsable du traitement
10. **Transmettre** ce registre tous les quatre mois à la CNPD
11. **Assister** à la rédaction des demandes d'autorisation auprès de la CNPD
12. **Définir** une politique de protection des données à caractère personnel
13. **Elaborer** des codes de conduites
14. **Contrôler** l'application de la politique, des procédures et autres codes de conduite spécifiques
15. **Exercer**, le cas échéant, son droit d'alerte (en interne et vis-à-vis de la CNPD)
16. **Etre** le lien privilégié avec l'autorité nationale (CNPD), mais aussi avec les personnes concernées
17. **Collaborer** avec les interlocuteurs internes clés (par exemple IT, RH, Marketing, lignes business, RSSI)
18. **Etre** le point de contact pour répondre aux demandes d'information et aux réclamations
19. **Apprécier** les mesures de sécurité prises, et ce, avec les personnes en charge de la sécurité des données
20. **Démontrer** une parfaite connaissance de la législation en matière de protection des données et en assurer la veille juridique
21. **Effectuer** le suivi des régularisations nécessaires et actions correctives
22. **Se concerter** avec le personnel du responsable du traitement pour convenir des actions à mener
23. **Gérer** les droits d'accès, d'opposition et d'information de toute personne concernée

Pouvoirs

Le DPO dispose des pouvoirs suivants:

⇒ un **pouvoir d'investigation** aux fins d'assurer la surveillance du respect de la législation sur la protection des données à caractère personnel par le responsable du traitement.

⇒ un **droit d'information** auprès du responsable du traitement concernant tout traitement de données à caractère personnel.

⇒ le **droit d'informer** le responsable du traitement sur les formalités à accomplir afin de se conformer aux dispositions de la législation luxembourgeoise sur la protection des données à caractère personnel.

Devoirs

Le DPO se doit de satisfaire aux devoirs suivants:

⇒ **Conseiller, assister et supporter** le responsable du traitement, afin de lui permettre de respecter la législation sur la protection des données à caractère personnel.

⇒ Participer à la **formalisation** et à la **mise à jour** des processus de traitement des données à caractère personnel

⇒ **Consulter** la CNPD en cas de doute quant à la conformité à la loi d'un traitement de données mis en œuvre sous sa surveillance

⇒ Jouer le rôle de **médiateur**, le cas échéant

⇒ **Enfin**, il est soumis au secret professionnel sans pour autant pouvoir l'opposer à la CNPD.

Quatre bonnes raisons pour désigner un Chargé de la Protection des Données Personnelles

1. Un facteur de sécurité juridique pour le responsable du traitement qui peut faire l'objet de sanctions pénales : le DPO facilite et participe à la mise en conformité des traitements avec la législation luxembourgeoise en matière de protection des données à caractère personnel.
2. Des échanges facilités et personnalisés avec la CNPD : le DPO est l'interface entre le responsable du traitement et la CNPD, grâce à son statut privilégié : celui-ci peut à tout moment échanger avec les agents de la commission.
3. La preuve d'un engagement éthique : La désignation d'un DPO montre l'engagement du responsable du traitement afin de respecter la vie privée et les droits des personnes concernées.
4. le DPO protège les intérêts du responsable du traitement et contribue à promouvoir une culture de la protection des données au sein de l'entreprise