**ANNEXE 4 : FICHE DE POSTE DE DELEGUE A LA PROTECTION DES DONNEES (DPO)**

*Ce modèle de fiche de poste est celui proposé par l’Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP).*

*Elle est disponible sur le site internet www.afcdp.net dans la rubrique « Carrières et emplois de DPO/CIL ».*

*Elle est en libre téléchargement.*

\* \* \*

**1. Présentation**

Le Délégué à la protection des données (DPD) ou *Data Protection Officer* en anglais (DPO) est une évolution du Correspondant à la protection des données à caractère personnel défini dans le titre III (articles 42 à 55) du décret n° 2005-1309 du 20 octobre 2005 pris pour l’application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés, plus connu sous l’appellation de Correspondant Informatique et Libertés (CIL).

Cette fonction de DPD est définie dans le Règlement général sur la protection des données (RGPD), 2016/679 du 27 avril 2016, principalement par le considérant 97 et par sa section 4. L’article 37 traite de la désignation du délégué à la protection des données, l’article 38 décrit ses fonctions et l’article 39 liste ses missions.

À partir du 25 mai 2018, les Délégués à la protection des données sont formellement désignés par les responsables de traitement auprès des autorités de contrôle (la CNIL en France), soit obligatoirement soit volontairement.

**2. Missions, activités et tâches**

La mission principale d’un DPD est de faire en sorte que l’organisme qui l’a désigné soit en conformité avec le cadre légal relatif aux données personnelles. La fonction de Délégué à la protection des données est un élément clé de co-régulation, par la pratique.

Cet objectif est atteint au travers des missions suivantes :

a) Informer et sensibiliser, diffuser une culture « Informatique et Libertés »

Le Délégué à la protection des données :

* mène ou pilote, de façon maîtrisée, des actions visant à sensibiliser la direction, les collaborateurs - dont le personnel participant aux opérations de traitement - aux règles à respecter en matière de protection des données à caractère personnel ;
* fait en sorte de présenter les efforts de mise en conformité comme productifs et positifs, et non comme seulement des contraintes ;
* s’assure que les personnes concernées sont informées des traitements opérés impliquant leurs données personnelles, ainsi que de leurs droits.

b) Veiller au respect du cadre légal

Le Délégué à la protection des données veille en toute indépendance au respect du Règlement européen (RGPD), d’autres dispositions du droit de l’Union ou du droit des États membres et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités. Ses analyses et conseils s’étendent aux sous-traitants et prestataires prenant part aux traitements décidés par le responsable de traitement.

Le DPD porte conseil auprès des directions Métiers concernées et, si besoin, auprès du Responsable de traitement, et émet des avis et recommandations motivés et documentés. Pour mener à bien ses tâches, le Délégué à la protection des données se fait communiquer par le Responsable de traitement l’ensemble des informations nécessaires et dispose des moyens adéquats.

Le Délégué à la protection des données est, notamment, étroitement associé aux sujets suivants :

* EIVP (Étude d’impacts sur la vie privée) ;
* « Privacy by Design » (prise en compte des impacts sur la vie privée dès la conception) ;
* notification des violations de données et communication aux personnes concernées.

Il est obligatoirement consulté avant la mise en œuvre d’un nouveau traitement ou la modification substantielle d’un traitement en cours et peut faire toute recommandation au Responsable de traitement.

c) Informer et responsabiliser, alerter si besoin, son responsable de traitement

Le Délégué à la protection des données informe sans délai le responsable de traitement de tout risque que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l’organisme et à ses dirigeants. À cette fin, il peut faire toute recommandation au Responsable des traitements et présenter des demandes d’arbitrage (il appartient au responsable de traitement de prendre la responsabilité de mettre en œuvre un traitement malgré les recommandations du DPD) Le professionnel veille à formaliser une procédure pour informer directement le Responsable de traitement d’une non-conformité majeure.

d) Analyser, investiguer, auditer, contrôler

Le Délégué à la protection des données mène, fait mener ou pilote, de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité de l’organisme, de mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.), de vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles.

e) Établir et maintenir une documentation au titre de « l’Accountability »

Le Délégué à la protection des données établit et maintient une documentation relative aux traitements de données à caractère personnel (dont le registre des traitements), au titre de la Responsabilité du Responsable de traitement (« Accountability ») et assure son accessibilité à l’autorité de contrôle.

f) Assurer la médiation avec les personnes concernées

Le Délégué à la protection des données reçoit les réclamations des personnes concernées par les traitements pour lesquels il a été désigné et veille au respect du droit des personnes. Il traite ces réclamations et plaintes avec impartialité, ou met en œuvre les procédures propres à assurer leur bon traitement.

g) Présenter un rapport annuel à son responsable de traitement

Le Délégué à la protection des données rend compte de son action en présentant chaque année un rapport à son Responsable de traitement. Ce rapport est le reflet fidèle de son action au cours de l’année écoulée et fait état des éventuelles difficultés rencontrées.

h) Interagir avec l’autorité de contrôle

Le Délégué à la protection des données est le point de contact privilégié de l’autorité de contrôle, avec laquelle il communique en toute indépendance sur les questions relatives aux traitements mis en œuvre par l’organisme qui l’a désigné, y compris la consultation préalable visée à l’article 36 du RGPD, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données peut exécuter d’autres missions et tâches. Dans ce cas, le responsable du traitement veille à ce que ces missions et tâches n’entraînent pas de conflit d’intérêts.

Le positionnement du DPD dans l’organisme est un facteur crucial de son efficacité et de la portée de ses actions.

Le DPD n’endosse pas la responsabilité juridique qui pèse sur le responsable de traitement concernant la conformité.

**Compétences**

Savoir

Aucun diplôme spécifique n’est exigé par le RGPD. Le métier est accessible à tous, du moment que le candidat possède les qualités professionnelles adéquates et, en particulier, des connaissances en technologies de l’information (pour pouvoir interagir avec les informaticiens et garder un esprit critique), des connaissances spécialisées du droit (ou une forte appétence pour ces sujets), mais également notamment sur les législations spécifiquement applicables à l’organisme (par exemple en matière de commerce électronique, de santé ou de travail) et des pratiques en matière de protection des données, ainsi que de qualités personnelles lui donnant une réelle capacité à accomplir ses missions.

Il est probable que les délégués à la protection des données désignés auprès de la CNIL dès mai 2018 soient d’anciens CIL confirmés dans leur position et, pour les nouveaux entrants, des personnes issues des métiers de la sécurité informatique, du droit, de la gestion du risque, de la conformité, ayant reçu les formations complémentaires indispensables.

Le niveau de connaissance n’est pas précisé par le RGPD, mais dépend de la sensibilité et de la complexité des traitements mis en œuvre par le responsable de traitement.

Le RGPD met l’accent sur le besoin de formation initiale et continue. Lorsque le Délégué à la protection des données ne dispose pas de l’ensemble des qualifications requises à la date de sa désignation, il doit les acquérir. Le Délégué à la protection des données se doit de maintenir ses compétences et connaissances dans ses domaines respectifs et de s’efforcer de les améliorer et de les enrichir constamment par la veille juridique, technologique et sociétale.

La pratique de la langue anglaise est un plus, afin d’être en mesure d’exploiter les nombreux documents et travaux uniquement rédigés dans cette langue.

Savoir-faire

Le Délégué à la protection des données doit maîtriser les techniques propres à son métier, concernant notamment l’analyse de conformité d’un traitement de données à caractère personnel, la formulation de conseils et d’exigences, la réalisation ou le pilotage d’audits afin de vérifier la conformité de traitements ou le respect de procédures ou de consignes, la conception et la réalisation d’actions de sensibilisation, la conception et la diffusion de procédures en lien avec la conformité au RGPD (traitement des demandes de droits des personnes, précautions à prendre en matière de contenu de zones de libre commentaire ou de cookies, détermination des durées de conservation, conception des mentions d’information des personnes, etc.), l’accompagnement d’un contrôle sur place de la CNIL, la préparation d’une demande d’avis ou d’autorisation auprès de la CNIL, la réalisation d’une EIVP, la gestion d’une notification de violation de données auprès de la CNIL et la communication aux personnes concernées, la formulation d’un bilan annuel, etc.

Le DPD démontre sa compétence et son professionnalisme dans l’accomplissement de ses missions. Il agit avec prudence et prend des décisions avisées dans toutes les situations de sa fonction.

Le Délégué à la protection des données base son jugement sur son expertise et son expérience.

Savoir-être, Qualités personnelles

Le Délégué à la protection des données fait preuve d’objectivité, d’indépendance, de probité et de discrétion. Il résiste au stress, aux influences indues et aux préjugés.

Objectivité : Les Délégués à la protection des données montrent un haut niveau d’objectivité lors de leur analyse, de l’évaluation et de toute communication auprès du responsable de traitement en ce qui concerne le niveau de conformité de ce dernier.

Ils réalisent leurs tâches en toute impartialité, c’est-à-dire qu’ils restent justes et sans parti pris dans toutes leurs actions. Ils font une évaluation équilibrée des informations et documentations reçues et forment leurs jugements sans être influencés par leurs propres intérêts ou par celui de tiers.

Indépendance : Le Responsable de traitement doit définir et faire connaitre les mesures garantissant l’indépendance du Délégué à la protection des données. Il doit imposer au Délégué à la protection des données de refuser toute ingérence dans son action et le met dans une situation qui lui permet de fait d’assurer cette indépendance (dont la mise à disposition de moyens).
Ainsi, le Délégué à la protection des données peut interagir directement et en toute indépendance avec le niveau le plus élevé de la direction et avec le Responsable du traitement ou son représentant, conformément à l’article 38 du RGPD.

Il n’a, dans son rôle de Délégué à la protection des données, aucun compte à rendre à un supérieur hiérarchique. Il dispose d’une liberté organisationnelle et décisionnelle dans le cadre de sa mission.

Il agit de manière indépendante, ne reçoit aucune instruction dans l’exercice de sa fonction et arrête seul les décisions s’y rapportant. Cette liberté ne signifie pas qu’il agit seul et sans concertation.
Il peut prendre contact avec quiconque (y compris la CNIL) dans le cadre de sa fonction.

Résistance au stress, aux influences indues et aux préjugés : Le Délégué à la protection des données doit pouvoir résister à toutes les influences que peuvent essayer d’exercer d’autres parties intéressées sur son jugement, ses analyses et conseils. Le principe d’objectivité s’impose à lui afin de ne pas compromettre ses jugements en raison de préjugés, de conflits d’intérêts ou d’autres influences indues.

Probité : Le Délégué à la protection des données agit en toute circonstance de façon diligente, loyale, responsable et honnête, en fonction de ses connaissances et de son degré d’expertise, au service du responsable de traitement pour lequel il agit.

Confidentialité et discrétion : Le Délégué à la protection des données est tenu au secret professionnel. Sous réserve des cas prévus ou autorisés par la loi, le DPD respecte une stricte confidentialité des informations, procédures, usages, plaintes et litiges dont il a connaissance dans le cadre de son activité.

Le DPO doit également être un « communicant », pour convaincre plutôt que contraindre.