RGPD, le Délégué à la Protection des Données de la fonction au métier

Comprendre et accompagner les entreprises et les salariés sur les enjeux d'emploi et de compétences

Descriptif fonction Délégué à la Protection des Données DPO

Délégué à la protection des données

Etude réalisée par l'AFPA dans le cadre de ses missions nationales de service public à la demande de la DGEFP.

SOMMAIRE

A. Contexte de l'étude P 3

B. Méthodologie P 3

C. Descriptif de la fonction de DPO P 4

1. Contexte d'émergence P 4

2. Conditions d'exercice P 4

3. Positionnement et autonomie dans l'organisation P 7

4. Les missions du DPO P 9

D. Annexes P 16

A. Contexte de l'étude

La Délégation Générale à l'Emploi et à la Formation Professionnelle (DGEFP) a mobilisé l'Agence pour la Formation Professionnelle des Adultes (AFPA) dans le cadre de sa mission de service public sur la thématique de la mise en œuvre du règlement général sur la protection des données (RGPD).

Cette initiative a reçu le soutien de la Commission Nationale de l'Informatique et des Libertés (CNIL), régulateur des données personnelles et de l'Association Française des Correspondants à la Protection des Données (AFCDP) afin de préciser et de promouvoir le métier de Délégué à la protection des données.

L'étude est composée de plusieurs parties :

B. Méthodologie

La description réalisée dans ce document est issue de plusieurs sources :

- le texte du RGPD, articles 37,38 et 39 (annexe 1)
- le référentiel de certification des compétences du DPO de la CNIL (annexe 2)
- la fiche de poste DPO de l'AFCDP (annexe 3)
- le modèle de lettre de mission AFCDP (annexe 4)
- la fiche fonction DPO du CNFPT (annexe 5)
- la charte de déontologie AFCDP (annexe 6)
- les résultats de l'enquête en ligne et les interviews de DPO

Nous illustrerons donc certaines parties par des résultats issus des réponses des 1265 DPO désignés auprès de la CNIL recueillies dans le questionnaire en ligne.

C. Descriptif de la fonction de Délégué à la Protection des Données (DPO)

1. Contexte d'émergence

Le Règlement Général sur la Protection des Données (RGPD), est un règlement qui encadre le traitement des données personnelles sur le territoire de l'Union européenne.
Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…). Ce nouveau règlement européen, entré en vigueur le 25 mai 2018 s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.
Le RGPD pose les règles applicables à la désignation, à la fonction et aux missions du Délégué à la Protection des Données (DPO).
Le DPO conseille et accompagne-le(s) organisme(s) qui le désigne(nt) dans la conformité avec le cadre légal relatif aux données personnelles.

2. Conditions d'exercice

Le DPO est désigné par son (ses) responsable(s) de traitement auprès de la CNIL, soit de façon obligatoire au titre de l'article 37 du RGPD, soit de façon volontaire.

Le DPO exerce ses missions dans des structures du secteur non marchand (administration, collectivité territoriale, association) ou marchand.

Illustration par des données issues de l'étude en ligne :

Tableau 1: Répartition du type d'organisation par typologie de DPO

		Ensemble DPO
Secteur non marchand 40.6 %	Organisme du secteur public ou assimilé	**10,2%**
	Administration publique ou une collectivité territoriale	**23,1%**
	Association	**7,3%**
Secteur marchand 59.4%	Entreprise privée	**39,6%**
	Cabinets conseil/ Indépendants	**17,6%**
	Autre	**2,2%**

A noter : parmi les répondants les DPO internes sont particulièrement présents dans les entreprises et les associations avec près de 60% des effectifs contre 41.2% pour les DPO mutualisés. Ces derniers exercent leurs fonctions à près de 58% dans une administration, une collectivité territoriale ou organisme du secteur public ou assimilés. Dans ces secteurs les DPO internes représentent 36.7%.

Les choix d'organisation de la fonction

En fonction des choix d'organisation de la ou des structures, il existe 3 typologies de DPO :

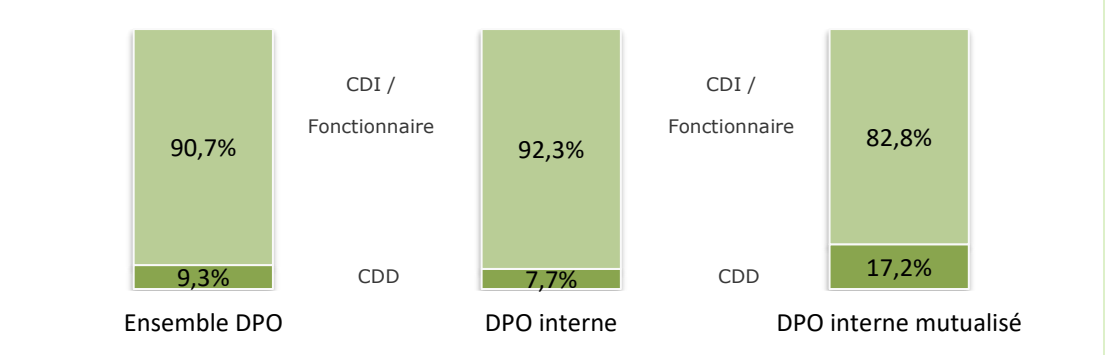
- Le DPO interne : salarié d'un seul responsable de traitement
- Le DPO interne mutualisé : salarié mutualisé pour plusieurs responsables de traitement
- Le DPO externe : indépendant, ou salarié d'un organisme spécialisé (cabinet de conseil, cabinet d'avocat…)

Les formes contractuelles

Le DPO peut exercer ses missions sous différentes formes contractuelles. Quand il est salarié le DPO bénéficie généralement d'un contrat à durée indéterminée ou d'un statut de fonctionnaire. Pour les DPO externes la contractualisation se fait sous la forme de contrat de prestation.

Illustration par des données issues de l'étude en ligne :

Graphique 1 : Répartition du type de contrat



Une large majorité des DPO internes et internes mutualisés sont sous statut contractuel en CDI ou fonctionnaires. Nous notons néanmoins que 9% d'entre eux exercent leurs fonctions en contrat à durée déterminée, ce taux atteint 17,2% chez les DPO internes mutualisés.

Le statut

Dans la grande majorité des cas, le DPO a un statut de cadre ou cadre supérieur.

Illustration par des données issues de l'étude en ligne :

Parmi les DPO internes et internes mutualisés, 85% répondent d'un statut de cadre ou cadre supérieur, les employés arrivent ensuite et représentent 9 % des effectifs.
Pour les DPO externes 28% exercent sous le statut de profession libérale, 22% en tant que salariés cadres ou cadres dirigeants, et près de 15% en tant que dirigeant.

Temps de travail alloué à la fonction

Il peut exercer ses missions à temps plein ou à temps partiel. S'il exerce d'autres fonctions dans la structure, cela ne doit pas entraîner de conflit d'intérêt.

Illustration par des données issues de l'étude en ligne :

Près de 70% des DPO occupent leurs fonctions à temps partiel.
Les DPO travaillant à temps complet ou à mi-temps et plus représentent 54.8 %.
Parmi les DPO travaillant à temps partiel :

- 41.5 % occupent cette fonction à moins de 25% de leur temps de travail
- 24.6% occupent cette fonction entre 26% et 49% de leur temps de travail
- 26.4% occupent leurs fonctions entre 50 et 69% de leur temps de travail
- 7.5% occupent leurs fonctions entre 70 et 95% de leur temps de travail.

Moyens

Le DPO peut travailler seul, disposer d'une équipe dédiée ou s'appuyer sur les moyens des services/directions informatique et juridique. Il peut, dans certaines organisations, s'appuyer sur un réseau interne de RIL (Relais Informatique et Libertés).

Le RGPD, sur la partie dédiée à la fonction de DPO (art 38), précise que le responsable de traitement doit fournir au DPO les ressources nécessaires pour l'exercice de ses missions. Il doit lui permettre l'accès aux données à caractère personnel et aux opérations de traitement.

Les DPO peuvent bénéficier d'un budget dédié ou solliciter des moyens auprès du responsable de traitement, et/ou généralement des services/directions informatique et juridique en fonction des enjeux de conformité.

Illustration par des données issues de l'étude en ligne :

Tableau 2 : Existence d'une équipe pour l'exercice de la fonction de DPO

	Ensemble DPO
Le DPO n'a pas d'équipe	75,0%
Le DPO dispose d'une équipe de 1 à 3 personnes	21,2%
Le DPO dispose d'une équipe de 4 personnes à 10 personnes	0,5%
Le DPO dispose d'une équipe de 4 personnes et plus	2,9%
Le DPO dispose d'une équipe de plus de 10 personnes	0,4%
Total	100,0%

Les trois quarts des DPO internes et internes mutualisés travaillent seuls. 21.1% d'entre eux disposent d'une équipe de 1 à 3 personnes pour les épauler.

64.9% des DPO internes et internes mutualisés ne disposent pas d'un réseau de RIL.

39.8% des DPO déclarent avoir un budget pour la mise en œuvre de leurs missions.

3. Positionnement et autonomie dans l'organisation

Le DPO doit avoir la capacité d'agir en toute indépendance. Il ne doit pas recevoir d'instruction dans le cadre d'exercice de ses missions.

Direction ou service de rattachement

Lorsqu'il est DPO interne ou interne mutualisé, il est généralement rattaché à la Direction générale ou Secrétariat général mais il peut aussi être rattaché à une direction juridique, informatique ou Service/Direction Conformité/Risques/Qualité. Ce rattachement doit veiller à ce que l'exercice de ses missions de DPO n'entraine pas de conflit d'intérêt avec ses autres missions dans la structure.

Illustration par des données issues de l'étude en ligne :

Tableau 3 : Service de rattachement du DPO

	Ensemble DPO
Service/Direction Conformité/Risques/Qualité	10,4%
Service/Direction générale/Secrétariat général	49,0%
Service/Direction informatique/Sécurité	16,5%
Service/Direction juridique	12,9%
Service/Direction Marketing	0,5%
Service/Direction Ressources humaines	2,6%
Service/Direction Sécurité/Sûreté	0,9%
Autre	7,3%
Total	100,0%

Près de la moitié, 49%, des DPO internes et internes mutualisés sont rattachés au service direction générale /secrétariat général. Viennent ensuite les directions informatiques avec 16.8% et les directions juridiques avec 12.9%.

Positionnement hiérarchique

Son positionnement dans l'organisation doit lui permettre de rendre compte de ses actions au plus haut niveau de la gouvernance de l'organisation et doit garantir son indépendance.

Illustration par des données issues de l'étude en ligne :

Globalement plus de la moitié des DPO, 53.4%, sont rattachés directement au responsable de traitement. Néanmoins, ils se répartissent de manière inégale avec 56.4% pour les DPO internes contre 39.3 % pour les DPO internes mutualisés.

11.7% des DPO internes mutualisés sont à une distance N-4 et plus de leurs responsables de traitement.

- **Responsabilité-sanction**

Le DPO ne peut être sanctionné pour l'exercice de ses missions. Le DPO ne peut être tenu responsable en cas de non-respect du règlement dans le traitement des données.

Le DPO est soumis au secret professionnel ou à une obligation de confidentialité dans le cadre de l'exercice de ses missions.

- **Respect de l'éthique professionnelle**

Le Délégué à la protection des données et le responsable de traitement/sous-traitant ont la possibilité de signer une charte de déontologie afin de promouvoir une culture de l'éthique parmi les Délégués à la protection des données désignés auprès de la CNIL au titre du RGPD.

4. Les missions du DPO

Le DPO conseille et accompagne-le(s) organisme(s) qui le désigne(nt) dans la conformité avec le cadre légal relatif aux données personnelles.

Dans le cadre de sa fonction, les missions du DPO peuvent être regroupées en trois grands domaines : le pilotage de la conformité, l'information et le conseil, le contrôle du respect de la réglementation.

Figure 1 : les missions du DPO

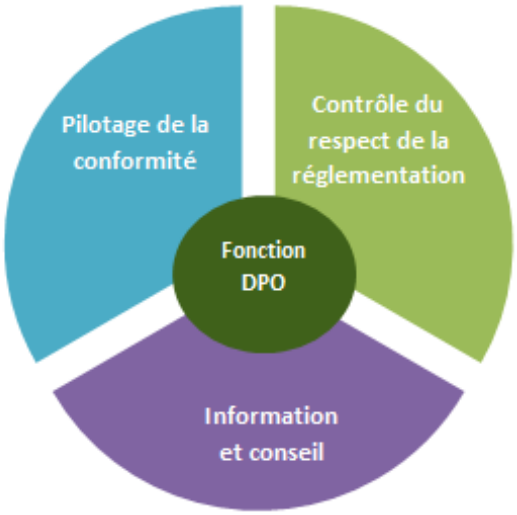


Figure 2 : les principaux interlocuteurs et niveaux de communication du DPO

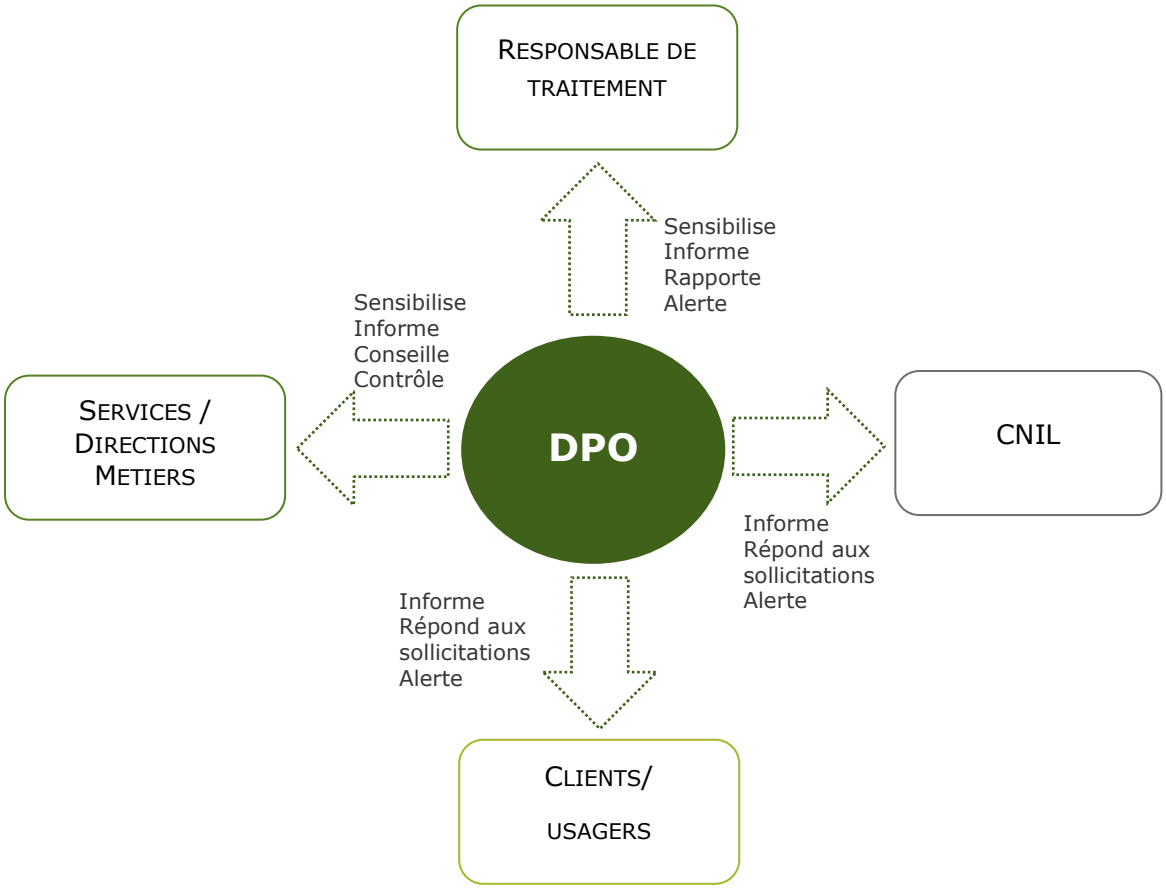
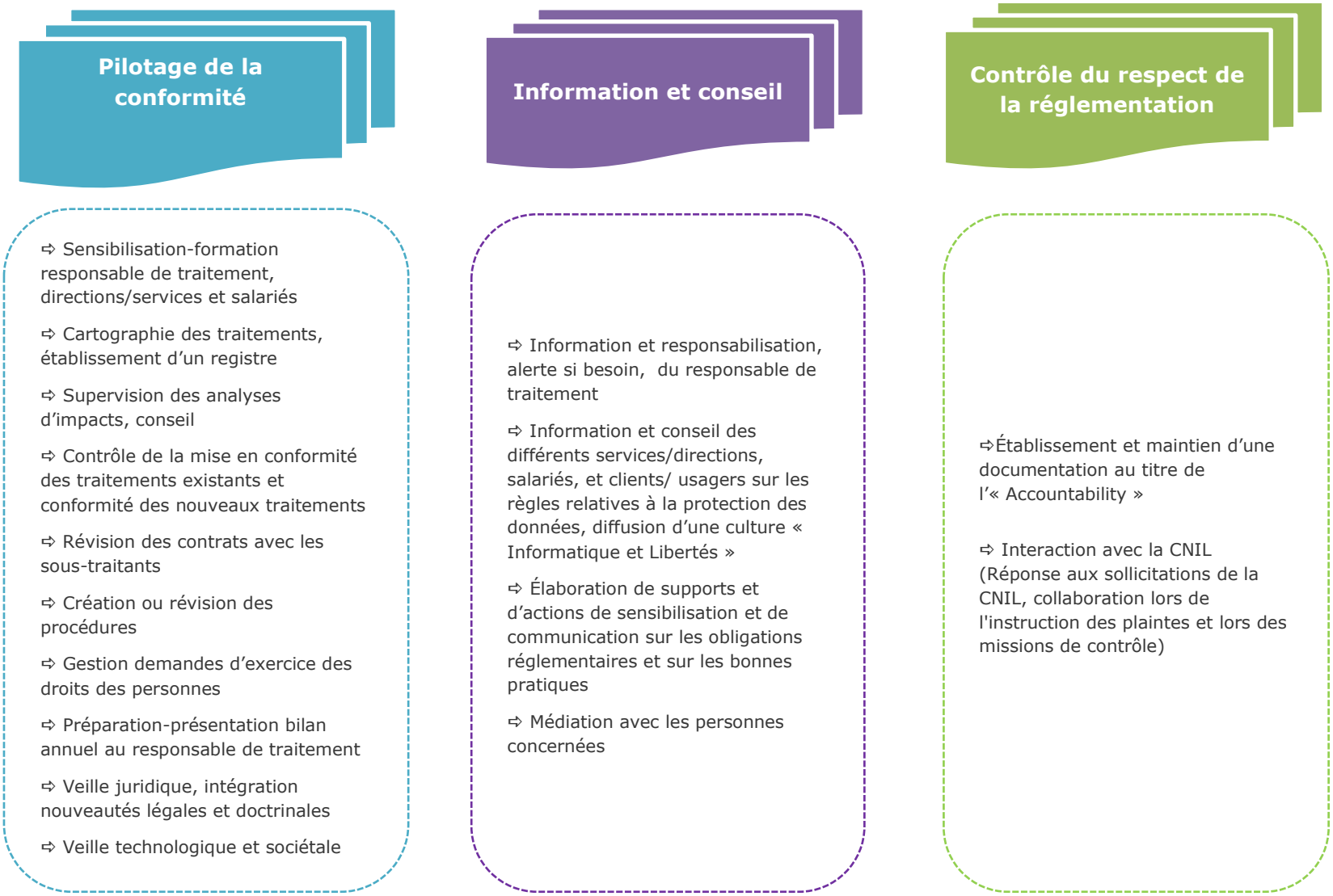


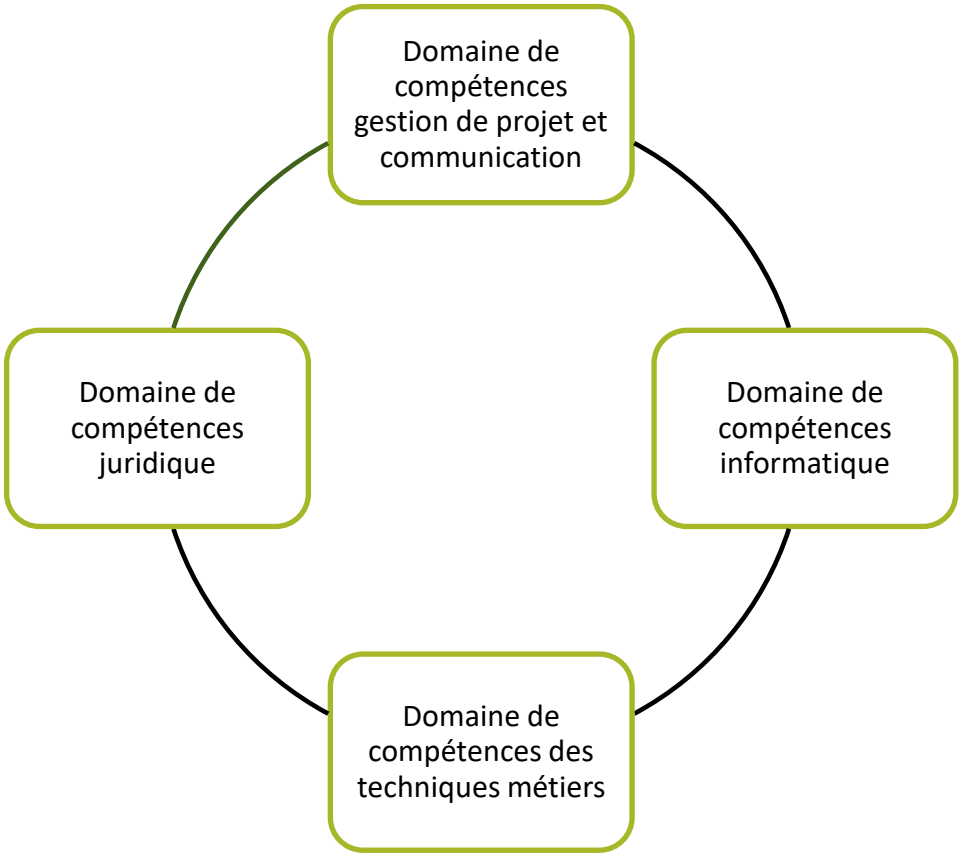
Figure 3 : les activités du DPO en fonction des missions



Pour mener à bien ses missions et réaliser ses activités, le DPO doit mettre en œuvre des compétences que l'on peut regrouper en 4 grands domaines :

- Le domaine de compétences de la gestion de projet et de la communication
- Le domaine de compétences des techniques métiers
- Le domaine de compétence juridique
- Le domaine de compétence informatique

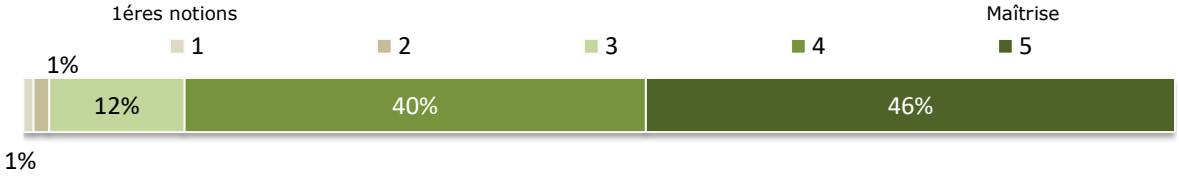
Figure 4 : les domaines de compétences du DPO



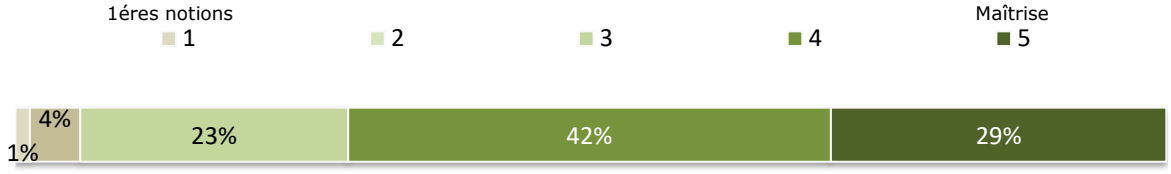
Nous vous présentons ci-dessous ces domaines de compétences avec le niveau de compétence requis perçu par les 1265 DPO ayant répondu au questionnaire en ligne.

- **Domaine de compétences gestion de projet et communication :**

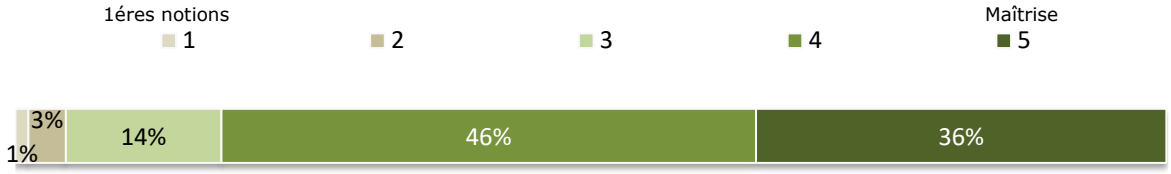
Capacités de communication et de pédagogie (former, faire comprendre, diffuser l'information)



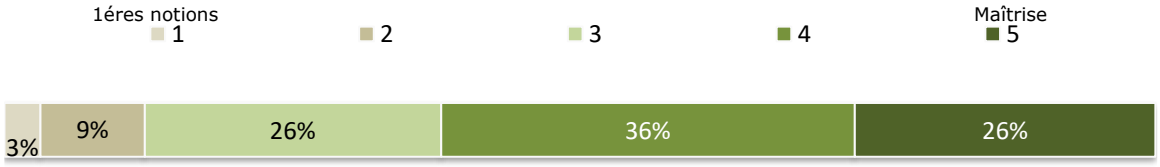
Capacité à négocier et convaincre



Capacités rédactionnelles

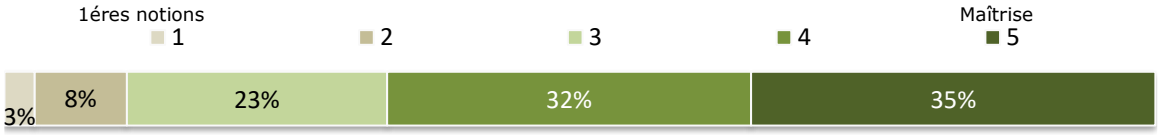


Compétences dans le domaine de la gestion de projet

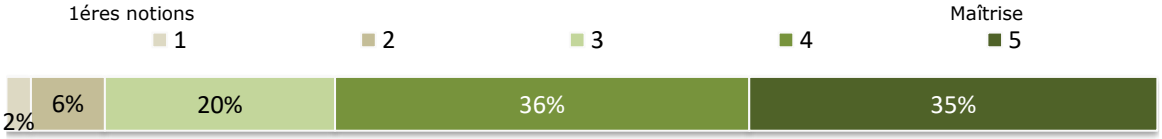


Domaine de compétences techniques métier

Compétences du métier DPO (savoir réaliser une analyse d'impacts, savoir formuler des mentions d'information, savoir gérer une violation de données, etc.)

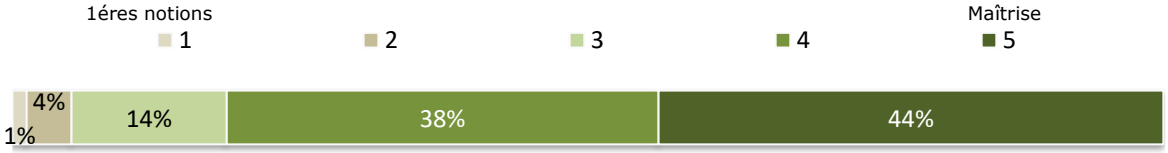


Connaissance du secteur d'activité dans lequel exerce le DPO

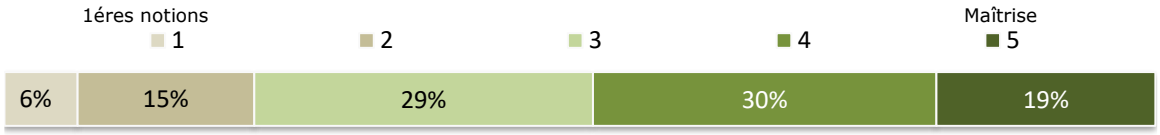


Domaine de compétences juridique

Compétences liées au cadre légal des données personnelles (RGPD, loi Informatique et Libertés)

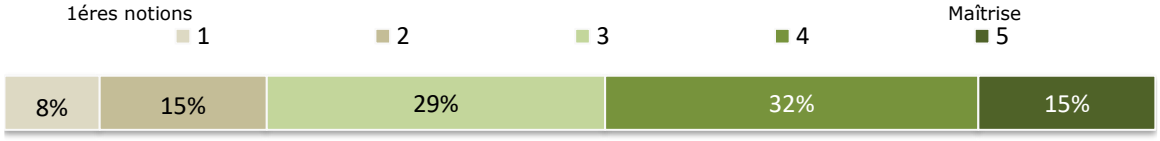


Compétences liées au cadre légal du secteur d'activité de la structure (Code du travail, Code de la santé publique, Code de la Sécurité Sociale, loi Cada, etc.)

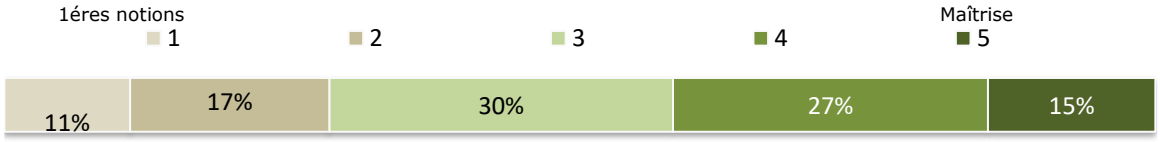


Domaine de compétences informatique

Compétences dans les systèmes d'information (flux, base de données, Cloud, cookies, etc.)

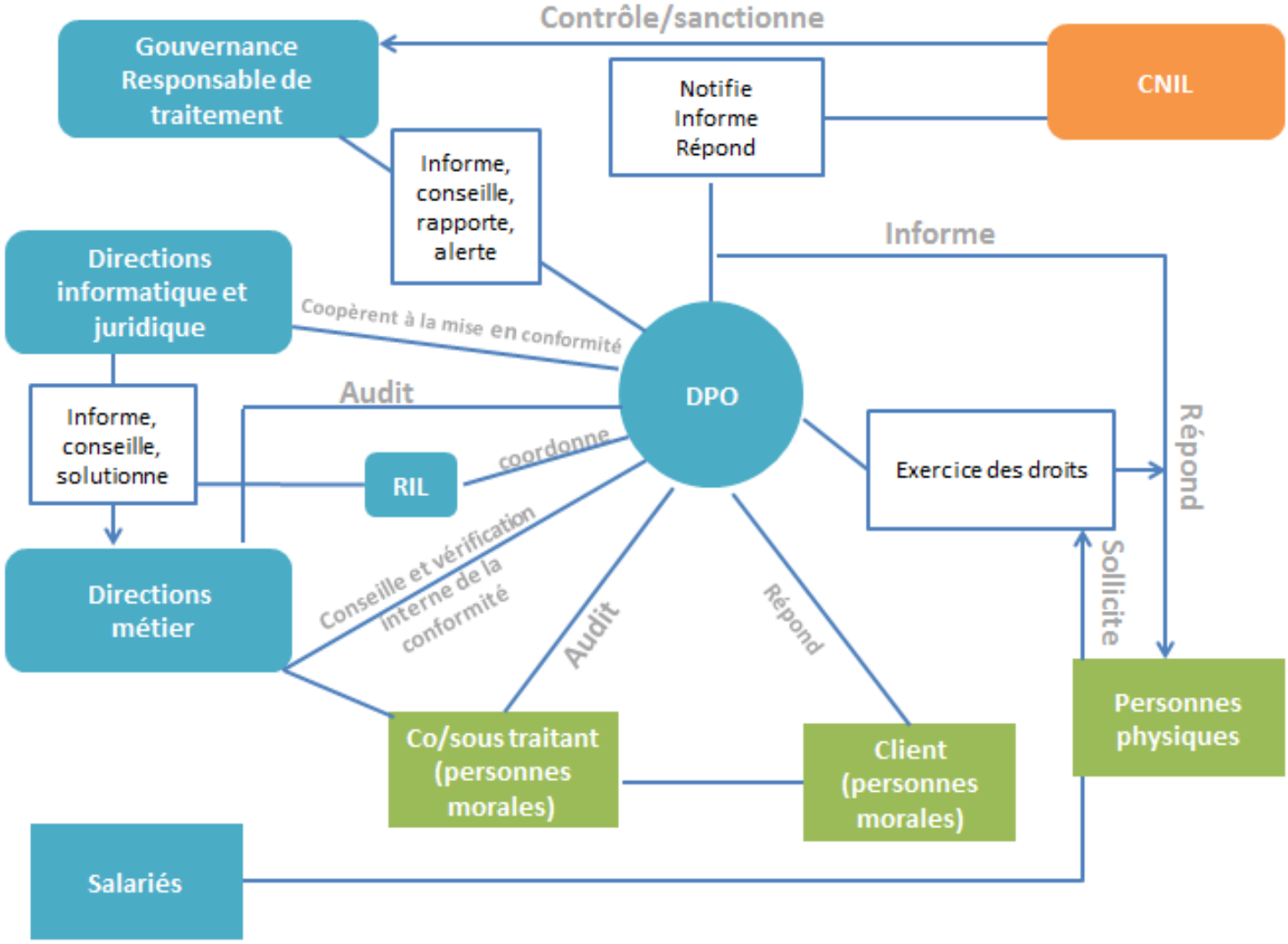


Compétences dans le domaine de la sécurité informatique (chiffrement, authentification forte, traçabilité, tests de pénétration, etc.)



La partie gestion de projet -communication apparait comme un domaine de compétence central dans l'exercice du métier de DPO. Cela peut s'expliquer par la nécessité pour la majorité des DPO de devoir articuler plusieurs domaines de compétences au sein de l'organisation et des directions métier. En effet, le DPO selon son parcours professionnel, ne détient pas un niveau d'expertise équivalent dans 2 des grandes composantes du métier à savoir les dimensions informatiques et juridiques. En ce sens, il doit être un médiateur entre les environnements professionnels des directions métiers, les exigences de conformité et l'opérationnalisation de leurs mises en œuvre. Il doit en cela, savoir repérer les criticités et faire appel aux ressources et compétences nécessaires pour mener à bien la mise en conformité.
Les dimensions de communication sont particulièrement présentes afin d'assurer la compréhension de la démarche et d'obtenir l'adhésion de l'organisation et de ses acteurs.

Figure 5 : environnement professionnel du DPO



D. Annexes

Annexe 1 : articles 37,38 et 39 du RGPD

Annexe 2 : le référentiel de certification des compétences du DPO de la CNIL

Annexe 3 : la fiche de poste DPO de l'AFCDP

Annexe 4 : le modèle de lettre de mission AFCDP

Annexe 5 : la fiche fonction DPO du CNFPT

Annexe 6 : la charte de déontologie AFCDP

Annexe 1 : RGPD CHAPITRE IV - Responsable du traitement et sous-traitant Section 4 - Délégué à la protection des données Articles 37 à 39

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4

Article 37 - Désignation du délégué à la protection des données

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

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.

Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Article 38 - Fonction du délégué à la protection des données

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 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 responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement.

Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.

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.

Article 39 - Missions du délégué à la protection des données

Les missions du délégué à la protection des données sont au moins les suivantes :

a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données 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, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;

d) coopérer avec l'autorité de contrôle ;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Annexe 2 : Référentiel de certification des compétences du délégué à la protection des données (DPO)

Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO) / JORF n°0235 du 11 octobre 2018 texte n° 51

https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=46002F5EFD8F35A73251FDC7949EEDB6.tplgfr26s_2?cidTexte=JORFTEXT000037485691&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037485359

RÉFÉRENTIEL DE CERTIFICATION DES COMPÉTENCES DU DÉLEGUÉ À LA PROTECTION DES DONNÉES (DPO)

Catégorie 1. Conditions préalables à remplir par le candidat à la certification

Exigence 1.1. Pour pouvoir accéder à la phase d'évaluation, le candidat remplit l'une des conditions préalables suivantes :

- justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles ; ou

- justifier d'une expérience professionnelle d'au moins 2 ans ainsi que d'une formation d'au moins 35 heures en matière de protection des données personnelles reçue par un organisme de formation.

Catégorie 2. Compétences et savoir-faire

Exigence 2.1. Le candidat connaît et comprend les principes de licéité du traitement, de limitation des finalités, de minimisation des données, d'exactitude des données, de conservation limitée des données, d'intégrité, de confidentialité et de responsabilité.

Exigence 2.2. Le candidat sait identifier la base juridique d'un traitement.

Exigence 2.3. Le candidat sait déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées.

Exigence 2.4. Le candidat sait établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées.

Exigence 2.5. Le candidat connaît le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles.

Exigence 2.6. Le candidat sait identifier l'existence de transferts de données hors Union européenne et sait déterminer les instruments juridiques de transfert susceptibles d'être utilisés.

Exigence 2.7. Le candidat sait élaborer et mettre en œuvre une politique ou des règles internes en matière de protection des données.

Exigence 2.8. Le candidat sait organiser et participer à des audits en matière de protection des données.

Exigence 2.9. Le candidat connaît le contenu du registre d'activités de traitement, du registre des catégories d'activités de traitement et de la documentation des violations de données ainsi que de la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données.

Exigence 2.10. Le candidat sait identifier des mesures de protection des données dès la conception et par défaut adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.11. Le candidat sait participer à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.12. Le candidat sait identifier les violations de données personnelles nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées.

Exigence 2.13. Le candidat sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données (AIPD) et sait en vérifier l'exécution.

Exigence 2.14. Le candidat sait dispenser des conseils en matière d'analyse d'impact relative à la protection des données (en particulier sur la méthodologie, l'éventuelle sous-traitance, les mesures techniques et organisationnelles à adopter).

Exigence 2.15. Le candidat sait gérer les relations avec les autorités de contrôle, en répondant à leurs sollicitations et en facilitant leur action (instruction des plaintes et contrôles en particulier).

Exigence 2.16. Le candidat sait élaborer, mettre en œuvre et est en capacité de dispenser des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données.

Exigence 2.17. Le candidat sait assurer la traçabilité de ses activités, notamment à l'aide d'outils de suivi ou de bilan annuel.

Annexe 3 : fiche de poste DPO de l'AFCDP

https://afcdp.net/dpo-fiche-de-poste-et-lettre-de-mission/

Exemple de fiche de poste d'un Délégué à la protection des données

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.

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.

Annexe 4 : lettre de mission DPO de l'AFCDP

https://afcdp.net/dpo-fiche-de-poste-et-lettre-de-mission/

Exemple de lettre de mission d'un Délégué à la protection des données

Madame, Monsieur,

(Nom de l'organisme) vous a désigné en tant que Délégué à la protection des données au titre du règlement (UE) 2016/679 du 27 avril 2016, le (JJ/MM/AAAA).

Cette désignation a fait l'objet d'un récépissé de la CNIL en date du (JJ/MM/AAAA) avec une date d'effet au (JJ/MM/AAAA).

Au titre de votre qualité de Délégué à la protection des données, vous êtes directement rattaché à [la Direction ou nom du DG, PDG, Maire …] et ne recevez aucune instruction pour l'exercice de vos missions.

Les instances représentatives ont été préalablement informées de la création de cette fonction par un courrier avec accusé de réception adressé le [date].

Vous exercez vos missions pour tous les traitements mis en œuvre par [Nom du ou des organismes responsables des traitements].

Par la présente, je vous précise quelles sont vos missions en tant que Délégué à la protection des données :

- m'informer et me conseiller – ainsi que l'ensemble de nos personnels - sur les obligations qui m'incombent en vertu du RGPD et d'autres dispositions en matière de protection de données à caractère personnel ;

- si besoin, m'informer des manquements constatés, me conseiller dans les mesures à prendre pour y remédier, me soumettre les arbitrages nécessaires ;

- veiller à la mise en œuvre de mesures appropriées pour nous permettre de démontrer que nos traitements sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;

- veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous nos projets comportant un traitement de données personnelles ;

- auditer et contrôler, de manière indépendante, le respect du RGPD par notre organisme, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement et les audits s'y rapportant ;

- piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et de la vie privée des personnes concernées ;

- vous assurer de la bonne gestion des demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées par nos traitements, vous assurer de leur transmission aux services intéressés et apporter à ces derniers votre conseil dans la réponse à fournir aux requérants ;

- être l'interlocuteur privilégié de l'Autorité de contrôle et coopérer avec elle ;

- dispenser vos conseils en ce qui concerne les études d'impact sur la vie privée et en assurer la pertinence ;

- mettre notre organisme en position de notifier d'éventuelles violations de données auprès de l'Autorité de contrôle et me porter conseil, notamment concernant les éventuelles communications aux personnes concernées et les mesures à apporter ;

- tenir l'inventaire et documenter nos traitements de données à caractère personnel en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;

- me présenter un bilan annuel de vos activités.

Pour vous permettre de mener à bien ces différentes missions, la Direction s'engage à :

- ce que vous soyez associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données ;

- vous aider à exercer vos missions en :

  - vous fournissant les ressources et moyens qui vous sont nécessaires ;
  - vous fournissant l'accès aux données et aux opérations de traitement ;
  - vous permettant d'entretenir vos connaissances spécialisées et vos capacités à accomplir vos missions, de réaliser votre veille et de vous tenir informé des meilleures pratiques propres à votre métier.

- veiller à ce que vous ne receviez aucune instruction en ce qui concerne l'exercice de vos missions et ne soyez pas relevé de vos fonctions ou pénalisé pour l'exercice de vos missions

- vous permettre de faire directement rapport au niveau le plus élevé de la direction

- veiller à ce que vos éventuelles autres missions et tâches n'entrainent pas de conflit d'intérêts avec celles relatives à votre qualité de Délégué à la protection des données ;

- donner une importance prépondérante à vos analyses et conseils en matière de protection des données personnelles et, dans le cas où vos recommandations ne seraient pas retenues, à en documenter les raisons ;

- s'assurer de votre avis avant mise en production de tout nouveau traitement comportant des données personnelles ;

- veiller à ce que vous poursuiviez une carrière normale au sein de l'organisme une fois votre mission terminée.

En fin de mission, vous vous engagez à me remettre tous les éléments relatifs à votre mission et, dans la mesure du temps dont vous disposerez à cet effet, à informer votre éventuel successeur sur les travaux en cours.

Je vous rappelle que vous êtes soumis au secret professionnel en ce qui concerne l'exercice de vos missions.

Une copie de cette lettre de mission sera portée à la connaissance de l'ensemble du personnel.

Je vous serais reconnaissant de bien vouloir me confirmer par courrier votre acceptation pour une telle mission accompagnée d'un exemplaire signé de la présente lettre.

Vos coordonnées seront rendues publiques. Il vous revient, par contre, de décider de la publicité de votre identité.

Je vous adresse tous mes encouragements et vous renouvelle ma confiance dans cette mission.

Je vous prie de croire, (Civilité), en l'assurance de ma parfaite considération.

(Prénom et nom du Responsable des Traitements)

Annexe 5 : fiche fonction du DPO CNFPT

http://www.cnfpt.fr/sites/default/files/fiche_fonction_deleguee_-_delegue_a_la_protection_des_donnees.pdf

FONCTION

DÉLÉGUÉE / DÉLÉGUÉ À LA PROTECTION DES DONNÉES

FAMILLE - FICHES FONCTIONS
DOMAINE D'ACTIVITÉS - FICHES FONCTIONS

FONCTION

Définition	**Pilote la mise en œuvre du règlement européen sur la protection des données pour le compte de la collectivité ou de l'établissement public. Informe, conseille les services et les agents sur l'application du règlement et en contrôle le respect. Vérifie l'exécution des analyses d'impact relatives à la protection des données. Il/elle est l'interlocuteur.trice de la Commission nationale informatique et libertés (CNIL) au sein de la collectivité ou de l'établissement public avec laquelle il/elle chargé.e de coopérer**
Facteurs d'évolution	• Transparence de la vie publique et ouverture des services et des données aux usagers • Développement de la mutualisation des SI et évolution des organisations • Développement de l'infogérance • Développements web et dépôt aux communautés libres • Dématérialisation des échanges internes et externes
Conditions d'exercice	• Cette fonction s'exerce par désignation de l'autorité territoriale, à temps complet ou à temps partiel • Désignation « sur la base des qualités professionnelles et, en particulier des connaissances spécialisées du droit et des pratiques en matière de protection des données, et de la capacité à accomplir ses missions » (article 37.5 du règlement européen) • La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel • Partage possible de la fonction entre plusieurs collectivités et établissements publics. Externalisation possible sur la base d'un contrat de service • Position dans l'organisation qui permet de garantir l'indépendance dans l'exercice de la fonction • Le/la délégué.e n'est pas responsable en cas de non-respect du règlement dans le traitement des données • Sens du relationnel et de l'écoute
Activités techniques	• Pilotage de la conformité aux règles relatives à la protection des données • Information et conseil relatifs aux obligations de la réglementation informatique et libertés • Contrôle du respect de la réglementation et des règles internes à la collectivité en matière de protection des données (notamment personnelles)

ACTIVITÉS/COMPÉTENCES TECHNIQUES

SAVOIR-FAIRE

Pilotage de la conformité aux règles relatives à la protection des données

- Assurer une veille juridique et diffuser une information sur les obligations de la collectivité ou de l'établissement public en matière de droits des personnes concernées par les traitements des données, au regard de l'évolution du droit informatique et libertés
- Informer les différents services de la mission de la déléguée/du délégué à la protection des données et identifier auprès d'eux des référents
- Identifier les sources (personnes, services) de traitements de données au sein de la collectivité
- Organiser des dispositifs de recensement des traitements de données
- Mettre en place une procédure d'échanges d'informations auprès des services pour toute évolution des modalités de traitement et pour tout nouveau traitement de données
- Rédiger des procédures de réalisation des analyses d'impact, de gestion des demandes des personnes concernées, de notification de non-respect de la réglementation
- Prioriser les actions à mener au regard des risques juridiques présentés par les traitements (protection, stockage et sécurité des données, conditions de communication, confidentialité...)
- Assurer la traçabilité de ses activités, rendre compte des actions engagées et des besoins complémentaires

Information et conseil relatifs aux obligations de la réglementation informatique et libertés

- Élaborer des supports et des actions de sensibilisation et de communication sur les obligations réglementaires et sur les bonnes pratiques
- Veiller à la présence des mentions d'information pour tout support de collecte de données
- Informer et conseiller les services, les agents et les usagers quant aux règles relatives à la protection des données

Contrôle du respect de la réglementation et des règles internes à la collectivité en matière de protection des données (notamment personnelles)

- Répondre aux sollicitations de la CNIL en particulier dans le cadre des consultations préalables à la mise en œuvre de traitements
- Apporter son concours à la CNIL à l'occasion notamment de l'instruction des plaintes et des missions de contrôle

SAVOIRS

> SAVOIRS SOCIOPROFESSIONNELS

- Droit de l'Union européenne et droit français en matière de protection des données, notamment personnelles
- Règles particulières de recueil et de traitement des données de la collectivité ou de l'établissement public
- Modes de traitement des données
- Conduite de projets informatiques
- Systèmes de gestion et d'exploitation de bases de données
- Politique de confidentialité et de sécurité des informations
- Tableaux de bord et indicateurs

> SAVOIRS GÉNÉRAUX

- Méthodes et techniques de concertation et de négociation
- Techniques de communication

Annexe 6 : charte de déontologie AFCDP

https://afcdp.net/media/documents/afcdp-charte-deontologie-du-dpo-approuvee-par-le-ca-19-avril-2018.pdf

CHARTE AFCDP DE DÉONTOLOGIE DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Approuvée par le Conseil d'administration de l'AFCDP le 19 avril 2018 (version 1.1)

1. Préambule 32
2. Dispositions générales 32
   2.1. Définitions 32
   2.2. Objet 33
   2.3. Approbation de la Charte 33
   2.4. Adhésion à la Charte - Champ d'application 34
   2.5. Diffusion - Publication 34
   2.6. Mise à jour de la Charte 35
3. La profession de Délégué à la protection des données 35
   3.1. Définition de la profession 35
   3.2. Missions du Délégué à la protection des données 35
      3.2.1. Participer à la conformité des traitements et veiller en toute indépendance au respect de la loi 36
      3.2.2. Établir et maintenir la liste des traitements (registre des activités) 36
      3.2.3. Analyser, investiguer, auditer, contrôler 36
      3.2.4. Fournir les recommandations et avertissements 37
      3.2.5. Informer et sensibiliser, diffuser une culture Informatique et Libertés 37
      3.2.6. Présenter un bilan annuel 37
      3.2.7. Être le point de contact et de coordination 37
      3.2.8. Alerter le cas échéant 38
      3.2.9. Soutien du Responsable de traitement/sous-traitant 38
      3.2.10. Accès au Délégué à la protection des données 38
4. Éthique du Délégué à la protection des données 40
   4.1. Qualités personnelles 40
      4.1.1. Probité 40
      4.1.2. Impartialité 40
      4.1.3. Compétences relationnelles 41
   4.2. Qualités professionnelles 42
      4.2.1. Secret professionnel 42

4.2.2. Conscience professionnelle – Professionnalisme 42
4.2.3. Compétences, connaissance, savoir-faire, savoir-être 42
4.3. Responsabilité du Délégué à la protection des données 43
4.4. Fin de mission 43
5. Relations du Délégué à la protection des données 43
5.1. Avec les personnes concernées 43
5.2. Avec le Responsable de traitement/sous-traitant 44
5.3. Avec le Donneur d'ordre 45
5.4. Avec les Autorités de contrôles 46
5.5. Avec les confrères 46

1. Préambule

Les données personnelles ne sont pas des données comme les autres et leur traitement implique une série d'obligations.

Les Délégués à la protection des données (souvent appelés DPO, pour *Data Protection Officer*), jouent un rôle important en tant que conseillers des responsables de traitements ou des sous-traitants, afin de veiller au respect des libertés et des droits fondamentaux des personnes concernées.

C'est dans cet esprit que l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP) a conçu la présente Charte de déontologie (ci- après désigné la Charte), afin de promouvoir une culture de l'éthique parmi les Délégués à la protection des données désignés auprès de la CNIL au titre du Règlement Général sur la Protection des Données (RGPD).

Ce document formule les règles de conduite qui doivent régir l'action de tout Délégué à la protection des données. La présente charte contribue donc à la bonne application du règlement 2016/679 du 27 avril 2016 et des lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243).

Les Délégués à la protection des données créent de la valeur : ils aident différents types d'organisations, publiques ou privées, à atteindre leurs objectifs stratégiques tout en protégeant leurs actifs immatériels et en veillant à la conformité des actions et processus avec la règlementation en vigueur sur la protection des données personnelles.

Par conséquent, il est nécessaire et pertinent que la profession se dote d'une Charte de déontologie, pour entretenir la confiance des organismes concernés envers ces professionnels et pour garantir la confidentialité, la qualité et le caractère intègre de leurs démarches et de leurs conseils.

Le Délégué à la protection des données contribue à la réduction des risques qui pèse sur les organismes. La Charte est donc également bénéfique aux responsables de traitements et aux sous-traitants, en ce qu'elle leur permet de savoir ce qu'ils peuvent attendre de leurs relations avec les professionnels, mais aussi du concours qu'ils doivent leur apporter afin de participer du succès de leur fonction et de leurs missions.

Par la signature de cette Charte, le Délégué à la protection des données prend des engagements forts. Mais ceux-ci s'appuient nécessairement sur le soutien du responsable de traitement ou du sous-traitant. C'est pourquoi cette Charte doit également être signée par ces derniers.

2. Dispositions générales

2.1. Définitions

AFCDP : Association Française des Correspondants à la protection des Données à caractère Personnel

Charte de déontologie : une charte de déontologie (ci-après « Charte ») régit un mode d'exercice d'une profession ou d'une activité en vue du respect d'une éthique. C'est un ensemble de droits et devoirs qui gouvernent une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public. Contrairement à un code de déontologie, une charte de déontologie n'est pas un document sanctionné par l'État, mais un texte rédigé et approuvé par les organismes qui défendent les intérêts d'une profession non règlementée.

Délégué à la protection des données (DPD, ou DPO, pour Data Protection Officer) : personne physique ou morale en charge de veiller au respect du RGPD, désigné officiellement par un responsable de traitement ou un sous-traitant auprès d'une autorité de contrôle, soit de façon obligatoire au titre de l'article 37 du RGPD, soit désigné de façon volontaire.

Déontologie : la déontologie (du grec deon, -ontos, ce qu'il faut faire, et logos, discours) est la science morale qui traite des devoirs à remplir.

Donneur d'ordres : personne physique ou morale qui bénéficie de la prestation d'un professionnel (concerne spécifiquement les DPO externes). La relation entre ces deux acteurs est définie par les dispositions régissant les relations au civil, administratives, commerciales ou de travail.

Loi « Informatique et Libertés » : Loi n°78-17 du 6 janvier relative l'informatique, aux fichiers et aux libertés, dans toutes ses versions modifiées.

Personne concernée : personne physique identifiée ou identifiable dont les données à caractère personnel font l'objet d'un traitement, selon les définitions de l'article 4 du RGPD.

Règlement européen ou RGPD : Règlement européen 2016/679 du 27 avril 2016 relatif la protection des personnes physiques l'égard du traitement des données à caractère personnel et la libre circulation de ces données (ci-après « RGPD »).

Responsable de traitement : personne physique ou morale qui détermine les finalités et les moyens du traitement, selon les définitions de l'article 4 du RGPD.

Sous-traitant : personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite les données pour le compte du responsable de traitement, selon les définitions de l'article 4 du RGPD.

2.2. Objet

Cette Charte a pour objet de donner des orientations quant à la conduite et au comportement des Délégués à la protection des données désignés auprès de la CNIL au titre du RGPD dans l'exercice de leur métier.

Cette Charte pourra s'intégrer au sein d'un ensemble de textes constituant des standards professionnels, comprenant notamment des guides de bonnes pratiques issues des lignes directrices publiées par le G29 – dont celui sur le DPO (*Data Protection Officer*).

2.3. Approbation de la Charte

La Charte est approuvée par vote à bulletin secret par le Conseil d'administration de l'AFCDP, sur proposition du Président.

La Charte est rendue publique par tout moyen, dont la publication sur le site web de l'association.

Elle prend effet un mois après sa publication, y compris en cas de modification.

2.4. Adhésion à la Charte - Champ d'application

L'adhésion à la Charte est volontaire, pleine et entière, gratuite et ne nécessite pas la qualité de membre de l'AFCDP.

Peuvent adhérer à la Charte :

- les Délégués à la protection des données internes (collaborateurs de l'organisme) ;
- les Délégués à la protection des données externes (personne physique ou représentant de la personne morale désignée), agissant en tant que prestataire ;
- les Délégués à la protection des données mutualisés (personne physique ou représentant de la personne morale désignée) désignés par plusieurs responsables de traitement ou sous-traitants.

La perte de la qualité de Délégué à la protection des données met fin d'office l'adhésion à la Charte.

Pour être valide, la Charte doit également porter la signature du Responsable de traitement ou du sous-traitant, ou de son représentant.

La présente Charte peut être invoquée par l'ensemble des Délégués à la protection des données (délégués désignés auprès de la CNIL) qui souhaitent s'en prévaloir l'égard d'un Responsable de traitement, d'un sous-traitant, d'un employeur, de partenaires internes et externes des organismes, de la CNIL, de confrères ainsi qu'à l'égard des personnes concernées au sens de l'article 4 du RGPD.

L'adhésion la Charte se fait simplement en adressant l'AFCDP un exemplaire portant les signatures du Délégué à la protection des données et du Responsable de traitement ou du sous-traitant qui l'a désigné. Un formulaire en ligne sur le site de l'AFCDP permet de matérialiser cet engagement et de communiquer leurs coordonnées afin d'être averti de toute évolution de la Charte. En apposant leurs signatures sur le document, le Délégué à la protection des données et le Responsable de traitement/sous-traitant prennent l'engagement d'en respecter les principes.

Cette adhésion peut se matérialiser par l'apposition d'un logo spécifique (téléchargeable sur le site web de l'AFCDP). Ce logo est la propriété intellectuelle de l'AFCDP et ne doit pas être utilisé de façon ostentatoire, notamment en termes de taille relative et d'occurrences. En aucun cas ce logo ne peut être interprété comme une garantie de qualité ou un jugement de valeur par l'AFCDP sur le professionnel qui l'arbore. À chaque fois que le logo est utilisé sur un site Web, un lien doit être établi vers la page qui présente le texte de la Charte afin que tous puissent prendre connaissance des engagements pris.

Sur le site web de l'AFCDP est publiée la liste des Délégués à la protection des données qui ont signé la charte, pour ceux qui le souhaitent.

2.5. Diffusion - Publication

La Charte peut, notamment, être :

- portée à la connaissance des personnes concernées ;
- mise à disposition au sein de tout organisme (auprès des IRP, auprès des salariés, etc.) ;
- annexée à un contrat de travail d'un Délégué la protection des données ;
- signalée comme document de référence dans le cadre de formations initiales et continues relatives aux métiers de la protection des données à caractère personnel ;
- référencée dans les contrats avec les clients et les mandants (pour un DPO externe) ;

- mentionnée par les recruteurs dans les offres de postes de Délégués à la protection des données ;
- présentée par un sous-traitant à un responsable de traitement pour justifier, avec d'autres mesures techniques et organisationnelles appropriées, qu'il présente des garanties suffisantes au sens de l'article 28 du RGPD.

2.6. Mise à jour de la Charte

Cette Charte sera révisée et mise jour par l'AFCDP. Des améliorations seront périodiquement réalisées pour l'adapter à la législation en vigueur et aux meilleures pratiques professionnelles.

Les mises à jour de la Charte sont rendues publiques par tout moyen à la discrétion du Président de l'AFCDP. Elles prennent effet auprès des personnes concernées, c'est-à-dire les Délégués à la protection des données et les Responsables de traitement/sous-traitant l'ayant signée, un mois après leur publication.

Les signataires de la Charte seront informés de ces mises à jour, à partir des coordonnées qu'ils auront communiquées lors de leur engagement en ligne. Par défaut et sans manifestation de leur part, les titulaires sont réputés maintenir le principe de leur adhésion aux règles édictées par la Charte. Si les titulaires ne se reconnaissent pas dans les modifications apportées à la Charte, ils se doivent d'en informer le Président de l'AFCDP et de retirer le logo de leurs supports.

3. La profession de Délégué à la protection des données

3.1. Définition de la profession

Dans le cadre de cette Charte, est considéré comme Délégué à la protection des données, tout « professionnel » personne physique ou morale désigné auprès de la CNIL au titre du RGPD via le formulaire de désignation disponible sur le site de la CNIL.

Si le Délégué à la protection des données est externe, il exerce une part majeure de son activité professionnelle dans tous les domaines liés à la conformité avec la règlementation applicable en France qui concernent la protection des données personnelles, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et la loi dite « Informatique et Libertés ».

Le document précise quand certaines règles de la Charte s'appliquent spécifiquement à certaines catégories de Délégué à la protection des données.

3.2. Missions du Délégué à la protection des données

Le Délégué à la protection des données doit :

a) Informer et conseiller son Responsable de traitement/sous-traitant ;

b) Veiller au respect du RGPD et de la loi Informatique et Libertés ;

c) Établir et maintenir (ou faire établir et maintenir) une documentation relative aux traitements de données à caractère personnel (dont le registre des traitements), au

titre de l'*Accountability*[1] et des lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243) ;

d) Analyser, investiguer, auditer, contrôler;

e) Fournir les recommandations et avertissements, demander des arbitrages si nécessaires ;

f) Informer et sensibiliser les personnels ;

g) Présenter un rapport annuel au représentant légal de l'organisme qui l'a désigné, au titre des recommandations des lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243) ;

h) Être le point de contact des personnes concernées et de la CNIL.

3.2.1. Participer à la conformité des traitements et veiller entoute indépendance au respect de la loi

Le Délégué à la protection des données doit veiller la conformité de l'ensemble des traitements mis en œuvre par le Responsable de traitement/sous-traitant, au RGPD, à la loi Informatique et Libertés et aux autres textes qui régissent la protection des données à caractère personnel en France.

À cette fin, il peut faire toute recommandation au Responsable de traitement/sous-traitant tant que toutes les conditions de leur licéité ne sont pas réunies.

3.2.2. Établir et maintenir la liste des traitements (registre des activités)

Le Délégué à la protection des données peut piloter la documentation que le Responsable de traitement/sous-traitant est tenu d'établir au titre de l'article 30 du RGPD et, notamment, dresser la liste des traitements de données à caractère personnel, comme le prévoient les lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243).

3.2.3. 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, d'objectiver les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.).

Pour mener à bien ces tâches, le Délégué à la protection des données se fait communiquer par le Responsable de traitement/sous-traitant l'ensemble des informations nécessaires et dispose des moyens et ressources nécessaires.

Le Délégué à la protection des données est, notamment, étroitement associé aux sujets suivants : EIVP (Étude d'impacts sur la vie privée) – comme le prévoient les lignes directrices sur les

[1] L'Accountability (ou responsabilité) désigne l'obligation pour les organismes de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données

DPIA (WP 248) adoptées par le Groupe de travail Article 29 –, *Privacy by Design* (prise en compte des impacts sur la vie privée dès la conception), Notification des violations de données.

3.2.4. Fournir les recommandations et avertissements

Le Délégué à la protection des données porte conseil auprès du Responsable de traitement/sous-traitant et émet des avis et recommandations motivés et documentés.

Il répond également aux demandes de renseignements et d'avis dont il est saisi. 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/sous-traitant.

3.2.5. Informer et sensibiliser, diffuser une culture Informatique et Libertés

Le Délégué à la protection des données :

- s'assure que les personnes concernées sont informées des traitements opérés impliquant leurs données personnelles, ainsi que de leurs droits ;
- mène ou pilote, de façon maîtrisée, des actions visant à sensibiliser la direction et les collaborateurs aux règles à respecter en matière de protection des données à caractère personnel ;
- veille à présenter les efforts de mise en conformité sous un jour favorable et positif, et en particulier propres à créer la confiance de la part des personnes concernées et la différentiation de l'organisme.

3.2.6. Présenter un bilan annuel

En tant que bonne pratique, héritée de la loi Informatique et Libertés dans sa version modifiée de 2004, le Délégué à la protection des données rend compte de son action en présentant chaque année un rapport à son Responsable de traitement, comme le prévoient, en tant que recommandation, les lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243). Ce rapport est le reflet fidèle de son action au cours de l'année écoulée et fait état des progrès et des éventuelles difficultés rencontrées.

3.2.7. Être le point de contact et de coordination

Le Délégué à la protection des données reçoit les questions des personnes concernées par les traitements mis en œuvre par le Responsable de traitement/sous-traitant et veille au respect du droit des personnes.

Il traite ces questions avec impartialité, ou met en œuvre les procédures propres à assurer leur bon traitement.

3.2.8. *Alerter le cas échéant*

Le Délégué à la protection des données informe sans délai le Responsable de traitement/sous-traitant ou le donneur d'ordre de tout risque que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir l'organisme et ses dirigeants.

Le professionnel veille à formaliser une procédure pour informer directement le Responsable de traitement/sous-traitant d'une non-conformité majeure.

3.2.9. *Soutien du Responsable de traitement/sous-traitant*

Afin de mener à bien sa mission, le Délégué à la protection des données doit :

- être informé en amont de tout projet impliquant des données à caractère personnel afin de pouvoir analyser sa conformité et formuler ses conseils. Il en sera de même à chaque étape du projet ;
- voir ses recommandations, étayées et développées, prises en compte. Dans le cas où ses recommandations ne seraient pas retenues, les raisons en seront documentées ;
- être à même de mener ou de piloter, de façon maîtrisée, toute action permettant de juger du degré de conformité de l'organisme, d'objectiver les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.). Pour mener à bien ces tâches, le Délégué à la protection des données se fait communiquer par le Responsable de traitement/sous-traitant l'ensemble des informations nécessaires pour tenir le registre des traitements/des catégories d'activités de traitements ou s'assurer qu'il est tenu conformément l'article 30 du RGPD ;
- être consulté préalablement à toute analyse d'impact relative à la protection des données et être même d'en vérifier l'exécution – voire de la réaliser. Si nécessaire, de préconiser la réalisation de telles analyses ;
- être étroitement impliqué dans tout ce qui concerne les notifications de violation de données (préparation, analyse des incidents et décision de notification à la CNIL et de communication aux personnes, analyse *a posteriori*, remise en cause des mesures prises pour sécuriser les données, etc.).

3.2.10. *Accès au Délégué à la protection des données*

- Le Délégué à la protection doit être joignable de manière simple et directe, que ce soit à l'intérieur de l'organisme dont il est Délégué ou par toute personne externe. À cet effet, ses coordonnées (telles que : adresse postale, téléphone, adresse de courrier électronique dédiée) seront communiquées par tout moyen approprié (intranet ou extranet ou encore site institutionnel par exemple). Le Délégué à la protection et le Responsable de traitement/sous-traitant peuvent également décider de publier de la même manière le nom du Délégué, comme le prévoient les lignes directrices sur les DPO adoptées le 5 avril 2017 par le Groupe de travail Article 29 (WP 243) ;
- Si le Délégué à la protection des données est mutualisé par un groupe d'entreprises ou d'organismes, il doit être facilement joignable à partir de chaque lieu d'établissement, que ce soit par les personnes concernées ou les autorités de contrôle,

mais également par chaque organisme dont il est Délégué à la protection des données. Il s'assure donc que ses coordonnées soient diffusées de manière appropriée ;

- Dans le cas d'un Délégué la protection intervenant dans plusieurs pays, ce dernier doit être en mesure de communiquer avec les personnes concernées et coopérer avec les autorités de contrôles dans la langue de ces dernières.

4. Éthique du Délégué à la protection des données

Les Délégués à la protection des données adhérant à la Charte se doivent :

- de se comporter avec honnêteté, exactitude, équité et indépendance ;
- d'offrir uniquement les services professionnels pour lesquels ils disposent de la pleine capacité d'exécution, d'informer de façon adéquate les responsables de traitement et les donneurs d'ordre sur la nature des missions assurées ou des services proposés, y compris toute préoccupation ou risque encouru ;
- de traiter de façon confidentielle toute information acquise au cours de relations professionnelles ;
- de donner priorité, dans toutes leurs actions et réflexions, à la protection des données personnelles des personnes concernées.

4.1. Qualités personnelles

4.1.1. Probité

Les Délégués à la protection des données agissent en toute circonstance de façon diligente, loyale, responsable et honnête, en fonction de leurs connaissances et de leur degré d'expertise, au service du Responsable de traitement/sous-traitant ou du donneur d'ordres pour lequel ils interviennent.

Par conséquent, les Délégués à la protection des données ne peuvent pas appliquer, dans l'exercice de leur métier, de méthodes illicites, ou contraires à l'éthique.

Les Délégués à la protection des données externes sont particulièrement vigilants quant à l'utilisation des noms, marques ou matériels documentaires des organismes qui les missionnent pour lesquels ils ont réalisé des prestations, dans le cadre d'utilisation de références commerciales, et veillent obtenir l'autorisation expresse des donneurs d'ordres avant toute utilisation.

4.1.2. Impartialité

L'impartialité est caractérisée par les éléments suivants : objectivité, indépendance, neutralité, équité, équilibre dans les jugements, absence de conflits d'intérêts, absence de préjugés, résistance aux influences abusives.

i) *Objectivité*

Les Délégués à la protection des données signataires de la Charte :

- montrent un haut niveau d'objectivité lors de leur analyse, de l'évaluation et de toute communication auprès du responsable de traitement ou du donneur d'ordres en ce qui concerne le niveau de conformité de ce dernier ;
- réalisent leurs tâches en toute impartialité, c'est-à-dire qu'ils restent justes et sans parti pris dans toutes leurs actions ;
- 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.

j) *Indépendance*

Le Responsable de traitement/sous-traitant doit définir et faire connaitre les mesures garantissant l'indépendance du Délégué à la protection des données. Il doit s'abstenir de toute ingérence et met le Délégué à la protection des données dans une situation qui lui permet de fait d'assurer cette indépendance, ce qui inclut 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/sous-traitant ou son représentant, conformément 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 est libre de consulter la CNIL ou tout sachant, dans la limite du cadre de sa fonction et de l'exercice de ses missions.

Concernant plus spécifiquement les Délégués à la protection des données à temps partiel, le Responsable de traitement/sous-traitant veille :

- à limiter les tâches qui incomberaient au Délégué à la protection des données au titre d'autres missions ;
- à s'assurer que le Délégué à la protection des données ne subisse pas de préjudices du fait de sa mission lors de l'étude annuelle de ses performances (gestion des ressources humaines) au titre de ses autres responsabilités ;
- à faire en sorte qu'une fois sa mission terminée, le Délégué à la protection des données poursuive, au sein de l'organisme, au moins la carrière qu'il aurait eue s'il n'avait pas occupé la fonction de Délégué à la protection des données.

De même, dans le cas d'un Délégué à la protection des données externe, le Responsable de traitement/sous-traitant doit s'abstenir de toute ingérence, notamment dans la perspective de l'éventuel renouvellement d'un contrat de travail ou de prestation. Le Responsable de traitement/sous-traitant ayant désigné un Délégué à la protection des données externe privilégie une durée de mission longue permettant de garantir cette indépendance.

k) *Absence et prévention de conflits d'intérêts*

Au-delà de la prévention des conflits d'intérêts au sens de l'article 38.6 du RGPD, le Délégué à la protection des données s'assure de l'absence de conflit de responsabilité dans ses missions.

Si le Délégué la protection des données n'exerce pas sa mission temps plein, ses autres missions et tâches ne doivent pas conduire ce qu'il prenne des décisions sur les traitements de données personnelles mis en œuvre par l'organisme.

En outre, le Délégué à la protection des données :

- ne peut être le prestataire de plus d'un client ou mandant dans une même affaire s'il y a conflit ou risque sérieux de conflit entre les intérêts de ses clients ou mandants ;
- s'interdit de s'occuper des affaires de tous les clients ou mandants concernés lorsque surgit un conflit d'intérêts, lorsque le secret professionnel risque d'être violé ou lorsque son indépendance risque de ne plus être entière ;
- ne peut accepter une mission confiée par un nouveau client ou mandant si le secret des informations données par un ancien client ou mandant risque d'être violé ou lorsque la connaissance des affaires de ce dernier favoriserait le nouveau client ou mandant ;
- se doit d'informer le Responsable de traitement/sous-traitant ou le donneur d'ordre de tous les intérêts qui pourraient influencer son jugement ou compromettre l'équité dont il doit faire preuve.

Les Délégués à la protection des données externes doivent prendre le soin d'évaluer en toute transparence avec les Responsables de traitement/sous-traitant concernés s'ils peuvent être désignés pour des organismes qui peuvent se considérer comme « concurrents ».

l) *Résistance aux influences abusives et aux préjugés*

Les Délégués à la protection des données sont sensibilisés à toutes les influences que peuvent essayer d'exercer d'autres parties intéressées sur leur jugement, leur anal se et leurs conseils. Le principe d'objectivité impose aux professionnels de ne pas compromettre leurs jugements en raison de préjugés, de conflits d'intérêts ou d'autres influences abusives.

4.1.3. Compétences relationnelles

Le Délégué à la protection des données veille à acquérir, développer et entretenir des qualités de communication, de négociation, de gestion des conflits.

4.2. Qualités professionnelles

4.2.1. Secret professionnel

Le Délégué à la protection des données est tenu au secret professionnel au titre de l'article 38.5 du RGPD.

Sous réserve des cas prévus ou autorisés par la loi, les professionnels respectent une stricte confidentialité des informations, procédures, usages, plaintes et litiges dont ils ont connaissance dans le cadre de leur activité.

Ils s'interdisent de faire tout usage de documents ou informations à caractère interne dont ils ont eu connaissance, dans l'exercice de leurs fonctions ou missions, chez un ancien Responsable de traitement/sous-traitant ou donneur d'ordre, sauf accord préalable exprès de ce dernier. De même, ils ne doivent pas utiliser de telles informations à des fins autres que celles définies par le donneur d'ordre.

Cette discrétion vaut auprès de l'environnement social du Délégué à la protection des données et se poursuit au-delà de la durée d'achèvement de la mission.

4.2.2. Conscience professionnelle – Professionnalisme

Le Délégué à la protection des données signataire de la Charte :

- démontre sa compétence et son professionnalisme dans l'accomplissement de ses missions ou prestations. Il agit avec prudence et prend des décisions avisées dans toutes les situations de sa fonction ;
- fonde son jugement sur son expertise et son expérience.

4.2.3. Compétences, connaissance, savoir-faire, savoir-être

Le Délégué à la protection des données doit avoir les connaissances, les compétences et l'expérience adéquates pour mener à bien sa mission et ses activités professionnelles. Le professionnel, candidat à un emploi de Délégué à la protection des données ou à une mission en tant que DPO, ne doit pas revendiquer une qualification qu'il ne détient pas ou une compétence qu'il ne maîtrise pas.

Le RGPD prévoit que le Délégué à la protection des données est une personne bénéficiant des qualifications requises pour exercer ses missions. Lorsque le Délégué à la protection des données est une personne morale, cette condition de qualification doit être remplie par le préposé désigné par celle-ci pour assurer les missions.

Ces compétences doivent porter tant sur l'informatique et les nouvelles technologies que sur la règlementation relative à la protection des données à caractère personnel. Elles doivent également avoir trait au domaine d'activité dans lequel il exerce ses fonctions.

Lorsque le Délégué à la protection des données ne dispose pas de l'ensemble des qualifications requises au moment de sa désignation, il doit les acquérir avant sa désignation.

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 et si besoin par une formation continue appropriée. Au titre de l'article 38.2 du RGPD, le Responsable de traitement/sous-traitant lui apporte son soutien dans ces efforts.

4.3. Responsabilité du Délégué à la protection des données

Au regard de la nécessaire indépendance dont le Délégué à la protection des données doit bénéficier et de l'absence de conflits d'intérêts qui doit être assurée, le Responsable de traitement/sous-traitant ne saurait valablement déléguer ses pouvoirs en matière de protection des données à caractère personnel au Délégué à la protection des données.

En outre, le Délégué à la protection des données ne peut être pénalisé ou relevé de ses fonctions par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions.

Comme tout salarié ou tout prestataire, le Délégué à la protection des données peut voir sa responsabilité civile délictuelle ou contractuelle, le cas échéant, et sa responsabilité pénale engagées dans les conditions du droit commun.

Le Délégué à la protection des données externe veille à souscrire à une assurance de responsabilité civile professionnelle couvrant l'ensemble des risques liés son activité.

4.4. Fin de mission

En fin de mission, le Délégué à la protection des données s'engage :

- à remettre au Responsable de traitement/sous-traitant ou donneur d'ordre tous les éléments en sa possession relatifs à sa mission ;
- dans la mesure du temps dont il dispose à cet effet, à informer son éventuel successeur sur les travaux en cours (pour un DPO externe, cela peut faire l'objet d'une facturation si non prévu dans sa prestation).

Lorsque le Délégué reste employé par l'organisme après la fin de sa mission, le Responsable de traitement/sous-traitant veille à ce qu'il poursuive au sein de l'organisme, au moins la carrière qu'il aurait eue s'il n'avait pas occupé la fonction de Délégué la protection des données

5. Relations du Délégué à la protection des données

5.1. Avec les personnes concernées

Le Délégué à la protection des données donne la priorité à la minimisation des risques pour les personnes concernées.

Dans toutes ses relations avec les personnes concernées, le Délégué à la protection des données se comporte de façon respectueuse et adaptée.

5.2. Avec le Responsable de traitement/sous-traitant

La relation entre le Délégué à la protection des données et le Responsable de traitement/sous-traitant est fondée sur la confiance et la franchise et exige que la démarche du professionnel soit intègre, honnête, fidèle et diligente.

Ainsi le Délégué à la protection des données concerné :

1. accepte une désignation en tant que DPO, uniquement s'il se juge compétent pour le faire, ce qui signifie qu'il dispose des connaissances et des ressources nécessaires afin d'exercer la fonction dans les meilleures conditions possibles. Dans les cas où il identifie une carence, il s'engage à solliciter du Responsable de traitement/sous-traitant les moyens adéquats et à acquérir les connaissances utiles avant sa désignation ;
2. dispose d'un accès facile et sans condition au Responsable de traitement/sous-traitant ou à son représentant direct et un rattachement au plus haut niveau de la hiérarchie ;
3. reçoit du Responsable de traitement/sous-traitant les moyens et ressources adéquates et nécessaires à la bonne réalisation de la fonction ou de la mission et de notifier clairement et sans délai tout défaut sur ce point ;
    a. informations et documentations suffisantes, pertinentes et fiables pour fonder ses conseils, conclusions et recommandations.
    b. accès facilité aux interlocuteurs, disposant des compétences et de l'autorité nécessaires, au sein de l'entreprise.
    c. assistance, formations, outils et budgets ;
    d. allègement sur d'autres tâches.
4. pilote la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et le respect des libertés et droits fondamentaux des personnes concernées par le Responsable de traitement/sous-traitant ;
5. porte à la connaissance du Responsable de traitement/sous-traitant, dans le cadre des missions et activités qui lui sont confiées, son évaluation du niveau de conformité de l'organisme. S'il a connaissance d'une non-conformité, le Délégué à la protection des données sera particulièrement attentif à en informer le Responsable de traitement/sous- traitant ;
6. rend compte au Responsable de traitement/sous-traitant et dans le cadre de sa mission, des points de non-conformité relevés et des risques encourus, et propose des mesures juridiques, organisationnelles ou techniques visant mettre en conformité l'organisme et à atténuer ou annuler les risques ;
7. s'engage à utiliser de façon confidentielle les informations et la documentation du Responsable de traitement/sous-traitant, à veiller à leur conservation sécurisée, et à ne pas les utiliser ni les conserver en dehors du strict cadre de sa mission.

Les Délégués à la protection des données ne peuvent agir seuls. Ils doivent développer des réseaux au sein de l'organisme dont ils assurent la conformité et cultiver les synergies avec le Responsable de la sécurité des systèmes d'information (RSSI), la Direction des Systèmes d'Information, la Direction juridique, les Directions métiers, etc.

5.3. Avec le Donneur d'ordre

La relation entre le Délégué à la protection des données externe et le donneur d'ordres est basée sur la confiance et la franchise et exige que la démarche du professionnel soit intègre, honnête, fidèle et diligente.

Ainsi le professionnel concerné :

1. s'interdit toute prospection de clientèle à l'aide de procédés ou de moyens allant à l'encontre de la dignité de la profession et susceptibles de porter atteinte à son image ;
2. veille ce que les contrats passés avec les donneurs d'ordres définissent précisément les conditions et moyens d'exécution de la prestation. Il veille en particulier à l'intégration, dans les contrats, des exigences de l'article du RGPD ;
3. s'interdit de donner à ses clients potentiels toute indication erronée quant à sa capacité et aux moyens tant humains que matériels dont il dispose (capacité à assurer la mission/la prestation). Il accepte une mission seulement s'il se juge compétent pour le faire, ce qui signifie qu'il dispose des connaissances et des ressources nécessaires afin d'exercer la fonction ou la mission dans les meilleures conditions possibles. Dans les cas où il identifie une carence, il en fait part à son interlocuteur pour trouver les moyens d'y remédier, notamment par un effort de formation complémentaire ;
4. se doit d'exiger du donneur d'ordres les moyens et ressources adéquats et nécessaires à la bonne réalisation de la fonction ou de la mission, et de notifier clairement et sans délai tout défaut sur ce point :
    a. informations et documentations suffisantes, pertinentes et fiables pour fonder ses conseils, conclusions et recommandations ;
    b. accès facilité aux interlocuteurs privilégiés, disposant des compétences et de l'autorité nécessaires, dans les différentes composantes de l'entreprise.
5. porte à la connaissance du donneur d'ordres, dans le cadre de la mission qui lui est confiée, de son évaluation du niveau de conformité de l'organisme. S'il a connaissance d'une non-conformité, le Délégué à la protection des données sera particulièrement attentif à en informer le donneur d'ordres ;
6. rend compte au donneur d'ordres et dans le cadre de sa mission, des points de non-conformité relevés et des risques encourus, et propose des mesures juridiques, organisationnelles ou techniques visant mettre en conformité l'organisme et atténuer ou annuler les risques ;
7. s'engage à utiliser de façon confidentielle les informations et la documentation du donneur d'ordres, et à veiller à leur conservation sécurisée ;
8. présente au donneur d'ordres des factures détaillées, transparentes et honnêtes, en évitant toute distorsion des montants, visant notamment à obtenir frauduleusement des primes ou des subventions ;
9. ne conserve pas les documents du donneur d'ordres en vue d'exercer un moyen de pression pour obtenir le recouvrement des factures relatives à ses missions.

5.4. Avec les Autorités de contrôles

Le Délégué à la protection des données :

- répond avec diligence à toutes les demandes de la CNIL ou d'une autre autorité de contrôle et défère aux convocations de celle-ci. Ses declarations auprès de celle-ci sont sincères ;
- entretient des relations loyales avec la CNIL et ses personnels ;
- est libre de prendre contact avec la CNIL en toute indépendance. Toutefois, s'il le juge nécessaire, il veille à en informer le Responsable de traitement/sous-traitant ;
- ne communique que le strict nécessaire concernant les activités du Responsable de traitement/sous-traitant dans le cadre de ses échanges avec l'Autorité de contrôle ;
- veille à la mise en place de procédures :
- lui permettant d'être informé de toute communication de la CNIL vers le Responsable de traitement/sous-traitant (communication de réclamations, demandes d'informations, contrôle sur pièces, convocation, etc.) ;
- lui permettant d'être informé de toute communication des services de l'organisme vers la CNIL.
- collabore loyalement à une mission de contrôle de la CNIL. Il permet, dans le respect des dispositions légales et réglementaires relatives à la protection de la vie privée et des secrets qu'elles protègent, la consultation, immédiate ou dans les plus brefs délais, de toute pièce réclamée, en version à jour. Il facilite la copie de ces pièces par les agents de contrôle et en informe le Responsable de traitement/sous-traitant.

5.5. Avec les confrères

La relation entre les Délégués à la protection des données est régie par les principes contenus dans la présente Charte.

Ces professionnels doivent, entre autres :

1. nouer des contacts avec leurs confrères pour favoriser les échanges d'expériences et la mise en commun des meilleures pratiques ;
2. entretenir entre collègues des relations basées sur le respect mutuel et la confraternité. Dans cet esprit, ils recherchent le règlement amiable de tout litige ;
3. ne pas discréditer ou dénigrer la profession, la présente Charte, leurs pairs ;
4. veiller au respect d'une concurrence loyale. Ils s'interdisent toute concurrence déloyale et toute entreprise de dénigrement tendant à nuire à un confrère ou à le supplanter de façon déloyale dans une mission qui lui a été confiée ;
5. s'assurer des intérêts généraux de la profession, et en particulier sa reconnaissance publique ;
6. s'investir dans la transmission de leur expertise auprès de stagiaires ou apprentis qu'ils pourraient accompagner ;
7. ne pas accepter de la part des Responsables de traitements/sous-traitant ou des donneurs d'ordres des conditions de travail qui sont impropres à la profession ou à

l'efficacité des missions, ni offrir ou imposer eux-mêmes de telles conditions de travail à leurs commettants ou propres partenaires.

Signatures (et cachet en sus pour l'organisme) :

	Le Délégué à la protection des données	Le Responsable de traitement/ sous-traitant
Date		
Signature (et Cachet pour l'organisme)		
Nom et prénom		
Adresse électronique		

☐ Oui, j'accepte que mon engagement à la « Charte AFCDP de déontologie des Délégués à la Protection des Données » soit mentionné sur le site web de l'AFCDP (www.afcdp.net), uniquement par l'indication de mon nom et de l'organisme pour lequel je suis désigné.

Les données à caractère personnel collectées dans le présent document font l'objet d'un traitement permettant de gérer les engagements à la Charte et sont conservées la durée nécessaire à cette finalité. Vous bénéficiez de droits d'accès, d'opposition, de modification, de limitation ou de suppression qui peuvent être exercés par courrier postal signé accompagné d'une copie de pièce d'identité signée adressé à « AFCDP - Délégué à la protection des données - 1, rue de Stockholm 75008 PARIS ».

Etude réalisée par l'AFPA Direction prospective métier dans le cadre de ses missions nationales de service public à la demande de la DGEFP.

Contact DGEFP

Dimitri Forges

Chargé de mission

Mission anticipation et développement de l'emploi et des compétences

Contacts AFPA

Alexandre BESNIER

Chargé de mission - Prospective métier

Nathalie DUBOURG

Consultante