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

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)
Texte disponible sur www.afcdp.net

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 1978 relative à 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 à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à 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 à 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 à 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 à la Charte se fait simplement en adressant à 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 à 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 à 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 nécessaire ;
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 en toute indépendance au respect de la loi

Le Délégué à la protection des données doit veiller à 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.).

[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.

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 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 à l'organisme et à 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 à l'article 30 du RGPD ;
- être consulté préalablement à toute analyse d'impact relative à la protection des données et être à 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 à 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 à 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.

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.

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 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 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.

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 à la protection des données n'exerce pas sa mission à temps plein, ses autres missions et tâches ne doivent pas conduire à 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 ».

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 analyse 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 à 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 à 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 à 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 à 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 28 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 à 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 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 déclarations 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 ».