CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

CRITÈRES DE CERTIFICATION DE DÉLÉGUÉ 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 5 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 3 ans** dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données, ainsi que d'une **formation d'au moins 60 heures** reçue et/ou dispensée par/avec des organismes de formation en matière de protection des données personnelles[1] ou
- 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, et d'une **formation d'au moins 100 heures** reçue et/ou dispensée par/avec des organismes de formation en matière de protection des données personnelles[2] ou
- justifier d'une **formation d'au moins 180 heures** reçue et/ou dispensée par/avec des organismes de formation en matière de protection des données personnelles[3].

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 l'existence de réglementation sectorielle qui fixe des conditions spécifiques au traitement de données.

Exigence 2.4 Le candidat sait déterminer les mesures appropriées pour fournir l'information requise aux personnes concernées.

Exigence 2.5 Le candidat sait établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées.

[1] Ces formations peuvent être celles labellisées ou certifiées par la CNIL dans le cadre de son référentiel en matière de formation relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
[2] Ces formations peuvent être celles labellisées ou certifiées par la CNIL dans le cadre de son référentiel en matière de formation relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
[3] Ces formations peuvent être celles labellisées ou certifiées par la CNIL dans le cadre de son référentiel en matière de formation relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Exigence 2.6 Le candidat connaît le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles.

Exigence 2.7 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 2.8 Le candidat sait élaborer et mettre en œuvre une politique ou des règles internes en matière de protection des données.

Exigence 2.9 Le candidat sait organiser des audits en matière de protection des données.

Exigence 2.10 Le candidat connaît le contenu du registre d'activités de traitement, du registre des catégories d'activités de traitement et du registre des violations de données ainsi que de la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données.

Exigence 2.11 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 2.12 Le candidat sait identifier des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.13 Le candidat sait identifier les violations de données personnelles nécessitant une notification à l'autorité de contrôle et une communication aux personnes concernées.

Exigence 2.14 Le candidat sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données et sait en vérifier l'exécution.

Exigence 2.15 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 2.16 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 2.17 Le candidat sait élaborer et mettre en œuvre des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données.

Exigence 2.18 Le candidat sait assurer la traçabilité de ses activités, notamment à l'aide de tableaux de bord ou d'outils de suivi.

1.1 Catégorie 3.Charte de déontologie

Exigence 3.1 La personne certifiée s'engage à respecter la charte déontologique figurant en **Annexe 1** du présent référentiel en la signant et en adressant la version signée à l'organisme de certification.

Annexe 1 : Charte de déontologie du DPO certifié conformément au référentiel de certification de DPO de la CNIL

Préambule

La présente charte constitue une déclaration expresse des valeurs, principes et règles qui doivent guider la conduite des personnes certifiées en tant que DPO conformément au référentiel de certification de DPO de la CNIL dans l'exercice de leurs missions en tant que DPO, ainsi que dans leurs relations avec d'autres employés, leurs clients, leurs prestataires, leurs fournisseurs, les institutions publiques ou privées et le public en général.

La charte regroupe des engagements concernant l'intégrité, l'impartialité, la confidentialité et la transparence que tout DPO certifié conformément au référentiel de la CNIL doit prendre en compte dans son activité de DPO.

Article 1 – Champ d'application

Les valeurs, principes et règles figurant dans cette charte doivent être appliqués par les DPO qui sont certifiés par les organismes de certification agréés par la CNIL conformément aux référentiels d'agrément et de certification de DPO de la CNIL.

Article 2 – Principes généraux

Le DPO certifié doit exercer son activité professionnelle conformément aux principes suivants :

- **Intégrité**, en respectant la réglementation en vigueur, notamment s'agissant des services qu'ils fournissent et en s'abstenant de toute activité illégale. Le DPO certifié ne doit pas utiliser sa certification de DPO pour d'autres usages que ceux liés à ses activités dans le champ de la certification délivrée.

- **Professionnalisme**, en exerçant sa fonction avec diligence et rigueur professionnelle et en maintenant ses connaissances constamment à jour.

- **Responsabilité et compétence** dans l'exercice de ses activités professionnelles, en exerçant les seules activités qu'il peut raisonnablement estimer pouvoir accomplir avec les connaissances et compétences nécessaires.

- **Impartialité**, en agissant de manière objective sans conflit d'intérêts qui pourrait remettre en cause son intégrité professionnelle ou celle de l'organisme pour lequel il exerce la mission de DPO.

- **Transparence**, en informant de manière claire, précise et suffisante son employeur ou ses clients de son rôle et de ses activités en tant que DPO par exemple par la présentation d'un bilan annuel.

- **Confidentialité**, en respectant et assurant la protection et la confidentialité des informations auxquelles il peut avoir accès en tant que DPO, en protégeant le droit à la vie privée de toutes les personnes concernées. De telles informations ne sauraient être utilisées pour un avantage personnel et ne sauraient être communiquées à des tiers non autorisés.

Article 3 – Relations avec l'employeur (si DPO interne) ou les clients (si DPO externe)

Dans ses relations avec son employeur ou ses clients, le DPO certifié :

- Doit informer du contenu de la présente charte.

- Doit agir de manière professionnelle dans le but de fournir un service de qualité et de développer une relation de long terme fondée sur la confiance.

- Doit toujours préserver son indépendance de toute influence par des liens économiques, familiaux ou d'amitié.

- Doit signaler à son employeur ou à son client tout conflit d'intérêts susceptible d'exister.

- Doit s'abstenir d'exercer une activité promotionnelle (publicité, matériel d'information, etc.) qui pourrait conduire ses clients ou prospects à une interprétation inexacte de la signification de la certification de DPO sur la base du référentiel de la CNIL.

- Doit mettre à la disposition de son employeur ou de ses clients un formulaire à compléter en cas de plainte ou de réclamation portant sur ses services fournis en tant que DPO. Ce formulaire sera adressé à la personne certifiée ou à l'organisme concerné par la plainte ou la réclamation et à l'organisme de certification.

Article 4 – Relations avec le personnel de son organisme

Dans ses relations avec les autres employés, dirigeants et collaborateurs de son organisme, le DPO certifié :

- Doit interagir de manière équitable et respectueuse.

- Doit s'abstenir de toute manifestation de harcèlement physique, psychologique ou moral et de tout abus de pouvoir.

- Doit superviser de manière adéquate leur activité sans dissimuler des erreurs ou des non-conformités et corriger toute non-conformité ou irrégularité détectée.

Article 5 – Relations avec les prestataires et les fournisseurs

Dans ses relations avec ses prestataires et fournisseurs, le DPO certifié :

- Doit établir des relations fondées sur la confiance, le respect et la transparence.

- Doit agir de manière impartiale et objective dans les procédures de sélection pour ces personnes en appliquant des critères de compétence, de qualité et de coûts, et en s'abstenant de tout conflit d'intérêts.

Article 6 – Collaboration avec les organismes de certification

Le DPO certifié collabore aux actions de supervision nécessaires au maintien et au renouvellement de la certification. Il informe l'organisme de certification de toute situation susceptible d'affecter sa certification.

Le DPO certifié collabore également avec l'organisme de certification concernant toute demande relative à une violation alléguée de la présente charte et pour résoudre toute plainte ou réclamation.

A cette fin, le DPO certifié tient un registre de toutes les plaintes et réclamations à son encontre concernant les activités exercées dans le champ de la certification de DPO et donne accès à ce registre à l'organisme de certification.

Dans les 10 jours suivant la réception de la plainte ou de la réclamation, le DPO certifié adresse une notification écrite et la copie de la plainte ou de la réclamation à l'organisme de certification.

Article 7 – Relations avec les autorités et administrations publiques

Le DPO certifié coopère avec les institutions, organismes et administrations publiques nationales et territoriales, en particulier avec la CNIL. Les notifications, injonctions et demandes d'information doivent être traitées avec diligence et dans le respect des délais fixés.

Article 8 – Exercice d'autres activités professionnelles

Le DPO certifié peut exercer d'autres activités professionnelles sous réserve que ces autres activités n'entraînent pas de conflit d'intérêts.

Article 9 – Acceptation et interprétation de la charte de déontologie

Le DPO certifié doit comprendre le contenu de la présente charte et s'engager à la respecter en la signant.

Toute question qu'il pourrait avoir sur l'interprétation et l'application de cette charte doit être adressée à l'organisme de certification qui est en charge de l'interpréter en cas de question et d'en assurer le respect.

Article 10 – Non-respect de la charte de déontologie

Le non-respect de l'un des principes, valeurs ou règles de la présente charte peut conduire à l'ouverture d'une enquête et à l'adoption de mesures disciplinaires prises par l'organisme de certification concerné (suspension ou retrait de la certification).