GUIDE PRATIQUE RGPD

DÉLÉGUÉS À LA PROTECTION DES DONNÉES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

L'objectif de ce guide est d'accompagner à la fois les organismes dans la mise en place de la fonction de délégué à la protection des données et ces délégués dans l'exercice de leur métier.

Ce guide est un outil vivant qui sera enrichi des bonnes pratiques remontées par les professionnels auprès de la Commission Nationale de l'Informatique et des Libertés.

TABLE DES MATIÈRES

AVANT-PROPOS

Le métier de délégué à la protection des données (« DPD », ou « DPO » dans ce guide) est devenu essentiel depuis l'entrée en application du règlement européen sur la protection des données (RGPD) le 25 mai 2018. Ce règlement, qui harmonise au niveau européen des obligations autrefois nationales, concerne les organismes dans toutes leurs activités : gestion des ressources humaines, prospection, relations avec la clientèle ou les usagers, etc. Désormais, le traitement de données personnelles est une composante fondamentale de la plupart des secteurs d'activité.

Il est ainsi naturel que le RGPD consacre trois de ses articles à définir les contours de la profession chargée de conseiller les responsables de traitement sur la protection de ces données. Dès lors, le DPO prend une importance qualitative et quantitative nouvelle par rapport à son prédécesseur en France, le correspondant Informatique et Libertés (CIL).

L'évolution est qualitative, tout d'abord : l'esprit du règlement est de **faire du DPO le « chef d'orchestre » de la gestion des données personnelles dans l'organisme qui le désigne**. Le positionnement hiérarchique du DPO doit en témoigner, et ses ressources doivent être adaptées, afin qu'il puisse accomplir pleinement son métier et son rôle de pilote de la conformité. Il ne doit pas travailler en vase clos, mais être pleinement intégré aux activités opérationnelles de son organisme. **Il est un maillon essentiel de la gouvernance de la donnée**, en lien avec le RSSI (responsable de la sécurité des systèmes d'information) et la DSI (direction des systèmes d'information).

Le métier de DPO s'est également transformé d'un point de vue quantitatif. Le nombre de DPO a en effet considérablement augmenté, du fait de **l'obligation de désignation** à laquelle sont soumis de nombreux organismes. Ainsi, alors que 18 000 organismes s'étaient dotés d'un CIL, **plus de 80 000 organismes avaient désigné un DPO en 2021**, dont 26 000 dans le public.

Pleinement consciente de cette évolution, la CNIL a adapté sa stratégie d'accompagnement des DPO, principalement en l'orientant sur le développement et le soutien de réseaux de délégués. Organisés par secteurs ou par régions, ceux-ci répondent à un premier niveau de questions du terrain, la CNIL n'intervenant que dans un second temps avec ces représentants et fédérations.

En complément de la page dédiée au DPO disponible sur le site web de la CNIL, ce guide a pour objectif d'accompagner à la fois les organismes dans la mise en place de la fonction de délégué à la protection des données et les DPO dans l'exercice de leurs missions.

Le guide du DPO s'articule en 4 chapitres :

- le rôle du DPO ;
- la désignation du DPO ;
- l'exercice des missions du DPO ;
- l'accompagnement du DPO par la CNIL.

Chaque thématique est illustrée par **des cas concrets et les questions fréquentes** en lien avec le sujet traité. Le lecteur peut également s'appuyer sur une FAQ et des outils pratiques, comme la lettre de mission.

Ce guide, dont la rédaction bénéficie de trois ans de pratique d'accompagnement des DPO, vous fournira les clefs pour tirer parti au mieux de la présence d'un délégué, être recruté en tant que DPO ou plus généralement faire évoluer votre conformité.

QUELLES SONT LES MISSIONS DE LA CNIL ?

En France, la Commission nationale de l'informatique et des libertés (CNIL) est l'autorité chargée de veiller à la protection des données personnelles. Elle poursuit quatre principales missions :

Informer et protéger les droits

La CNIL répond aux demandes des particuliers et des professionnels. Elle mène des actions de communication auprès du grand public et des professionnels que ce soit à travers ses réseaux, la presse, son site web, sa présence sur les réseaux sociaux ou en mettant à disposition des outils pédagogiques.
Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Accompagner la conformité et conseiller

Afin d'aider les organismes privés et publics à se conformer au RGPD, la CNIL propose une boîte à outils complète et adaptée en fonction de leur taille et de leurs besoins.
La CNIL veille à la recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

Anticiper et innover

Pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée, la CNIL assure une veille dédiée.
Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de *privacy by design*.

Contrôler et sanctionner

Le contrôle permet à la CNIL de vérifier la mise en œuvre concrète de la loi. Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amende, etc.).

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Les missions de la CNIL
- Statut et organisation de la CNIL.

LE RÔLE DU DPO

Le RGPD place le DPO en acteur clé du système de gouvernance des données personnelles. En effet, les missions qui lui sont attribuées consacrent son rôle de pilote de la démarche de mise en conformité permanente et dynamique dans laquelle les organismes doivent s'inscrire.

FOCUS : LES TEXTES DÉFINISSANT LA FONCTION DE DPO

La fonction de DPO est réglementée et définie avec précision dans les articles 37 à 39 du RGPD. Ce guide s'appuie sur ce règlement, la loi Informatique et Libertés et son décret d'application, ainsi que les lignes directrices sur le DPO du Comité européen de la protection des données (CEPD). À la fin de chaque partie, un renvoi vers les passages pertinents de ces textes sont indiqués.

Conseiller et accompagner l'organisme

Le DPO a un rôle de conseil et d'accompagnement à plusieurs niveaux :

- il apporte son expertise auprès de la direction afin que celle-ci puisse assurer la conformité des traitements ;
- il diffuse la culture et les règles de la protection des données auprès de toutes les personnes qui traitent des données personnelles au sein de l'organisme.

Le DPO peut ainsi identifier et formaliser les moments clefs à l'occasion desquels il **souhaite que son intervention ou sa présence soit systématique**, par exemple pour chaque :

- projet de décision de création ou d'évolution d'un traitement existant (afin notamment de veiller au respect des principes de protection des données dès la conception et par défaut) ;
- examen de la nécessité de réaliser une analyse d'impact relative à la protection des données (AIPD) et réalisation effective de celle-ci ;
- rédaction ou tenue du registre des activités de traitement ;
- rédaction et mise à jour des règles ou politiques internes en matière de protection des données ;
- violation de données personnelles, afin de conseiller sur les mesures à prendre ainsi que sur la notification à l'autorité et aux personnes concernées.

Le DPO sensibilise et accompagne les acteurs impliqués au sein de chaque service traitant des données :

- en veillant à l'adoption par tous d'une culture « protection des données personnelles » (par

exemple via des formations internes sur les grands principes de la protection des données) ;

- en procédant à des actions de communication et de sensibilisation sur des sujets pertinents pour l'organisme (utilisation d'affiches et guides pratiques accessibles depuis l'intranet, rappel des règles de sécurité à l'occasion d'une sanction ou d'une violation de données citée dans les médias, fausses campagnes de « *phishing* » à but éducatif, etc.) ;
- en se présentant comme l'interlocuteur interne référent pour toute question en matière de protection des données, et si nécessaire au moyen de personnes relais.

Le DPO a donc avant tout une mission d'information, de conseil et de contrôle. **Il n'est pas responsable de la conformité de l'organisme**, de la tenue du registre, de la réalisation des analyses d'impacts ou des notifications de violations de données. Il est cependant en position d'en être un acteur clef dont les compétences seront très utiles au responsable de l'organisme pour l'aider à se conformer à ses obligations.

FOCUS : LE PILOTAGE DE LA CONFORMITÉ PAR LE DPO

Veiller à la conformité au RGPD est une démarche active qui consiste à anticiper et organiser les interventions du DPO au sein de l'organisme.
Les démarches à mettre en place peuvent par exemple être les suivantes :

- formaliser les cas de consultation du DPO ;
- mettre en place, auprès des directions concernées un « comité RGPD » chargé d'arbitrer et d'orienter les actions concernant les traitements de données ;
- être associé à l'élaboration et à la mise à jour des documents de gouvernance (politique de sécurité du système d'information, charte informatique, livret d'accueil, règlement intérieur, etc.) ;
- entretenir un contact régulier avec les opérationnels qui traitent des données personnelles, être à leur écoute et en soutien ;
- prévoir une procédure interne en cas de contrôle de la CNIL (modalités d'accueil, personnes à prévenir, informations à obtenir), de violation de données personnelles (information immédiate au DPO), ou de blocage interne (alerte du responsable de traitement et/ou résolution du conflit) ;
- prévoir les modalités de réponse aux demandes extérieures (rédiger des modèles de réponse, informer les services en relation avec le public) ;
- prévoir une personne relai en cas d'absence ou d'empêchement qui peut recevoir les demandes et être le point de contact en interne vis-à-vis des personnes concernées mais aussi de la CNIL ;
- identifier les services pertinents pour les démarches d'animations et de formations régulières, en s'aidant, si besoin, de relais internes ou externes compétents ;
- tenir un tableau de bord des activités menées, afin d'alimenter un point régulier (réunion de direction) ainsi qu'un rapport d'activité régulier à destination de la direction de l'organisme ;
- être acteur de son réseau professionnel en identifiant et en collaborant avec les interlocuteurs pertinents de l'organisme (relais internes, responsables conjoints de traitement, prestataires) ;
- entretenir ses connaissances techniques et opérationnelles en lien avec les activités de traitement de l'organisme à travers une veille (sur la jurisprudence, les publications des autorités de contrôle, etc.) et à l'occasion de formations et de partages d'expérience (réseau géographique et/ou professionnel de DPO).

Contrôler l'effectivité des règles

Le DPO est investi d'une mission de contrôle du respect du RGPD.

Cette mission doit prendre la forme de vérifications organisées par le DPO (audit externe ou relais interne), ou menées par le DPO personnellement, en collaboration avec les autres fonctions clefs telles que le RSSI (responsable de la sécurité des systèmes d'information). Elle doit s'accompagner d'un suivi du plan d'actions correctives et évolutives.

En fonction des priorités, l'objet de ces contrôles ou audits peut consister en :

- des vérifications de l'exactitude des informations contenues dans le registre des traitements mis en œuvre par l'organisme (inventaire des activités de traitement, périmètre des finalités, personnes concernées, nature des données traitées, destinataires et éventuels transferts hors de l'Union Européenne, durées de conservation, mesures de sécurité) ;
- des vérifications de la conformité des traitements les plus sensibles, en prenant en compte les analyses d'impact effectuées (notamment s'agissant de la mise en œuvre des mesures censées diminuer la vraisemblance et la gravité des risques) ;
- la mise en place d'outils de suivi et de contrôle de l'utilisation des traitements (analyse de logs, détection de données interdites, vérification du respect des durées de conservation, etc.) ;
- un contrôle de l'effectivité des mesures techniques et organisationnelles de protection des données que l'organisme s'est engagé à mettre en œuvre.

Être le point de contact de l'organisme sur les sujets RGPD

Avec la CNIL

Le DPO est, d'une part, amené à coopérer avec l'autorité de contrôle et doit à ce titre jouer un rôle de « facilitateur » à l'occasion des échanges avec la CNIL (réponse aux demandes lors d'un contrôle sur place, instruction d'une réclamation, consultation dans le cadre d'une AIPD, notification d'une violation de données, etc.).

Par ailleurs, le DPO peut consulter la CNIL sur toutes questions ayant rapport avec la protection des données personnelles ou sa fonction. Il est interdit au responsable de traitement ou au sous-traitant de soumettre ces questions à sa validation ou de les prohiber.

En outre, selon la Charte d'accompagnement des professionnels qu'elle a publiée en février 2021, **la CNIL ne répond pas aux demandes de conseils qui lui sont adressées par des organismes n'ayant pas pris le soin de consulter leur DPO** sur la question qu'ils souhaitent poser.

La majorité des contrôles sur place de la CNIL sont inopinés. Toutefois, exceptionnellement, l'organisme et le DPO peuvent en être avertis quelques jours auparavant. Le DPO peut, lors d'un contrôle sur place, être « responsable des lieux » où se situent le ou les traitements qui font l'objet des vérifications. Il est alors l'interlocuteur privilégié, mais pas exclusif, de la délégation de contrôle et est chargé de la relecture et de la signature du procès-verbal dressé à la fin de la journée. Le responsable de traitement reste en capacité de faire ses observations sur le procès-verbal lorsqu'il lui sera adressé.

En revanche, le DPO ne peut pas représenter seul l'organisme auprès de la CNIL lors d'une audition sur convocation, car cela le mettrait en situation de conflit d'intérêts. Il peut néanmoins accompagner un représentant de l'organisme pour apporter son expertise et répondre aux questions.

Avec les personnes concernées par les traitements de données personnelles

Le DPO est également le point de contact des personnes dont les données sont traitées par l'organisme qui l'a désigné. À ce titre, il peut prendre en charge l'organisation du traitement de leurs demandes d'exercice de droits (accès, portabilité, etc.) afin qu'une réponse complète soit apportée dans les délais impartis. Le DPO peut également être sollicité par les personnes concernées (salariés, agents, clients, fournisseurs, étudiants, usagers, etc.) au sujet de toute question relative au traitement de leurs données personnelles.

ATTENTION

Dans le cadre d'une réponse à une plainte, le DPO agit comme point de contact avec la personne concernée et les agents de la CNIL. **Cela ne l'autorise pas à communiquer les coordonnées directes des agents de la CNIL à des tiers** (y compris la personne concernée). Ces coordonnées sont destinées au seul destinataire des messages envoyés et à ses collaborateurs.

Assurer la documentation des traitements de données

La documentation tient un rôle prépondérant dans la nouvelle logique de responsabilisation (ou redevabilité, ou encore « *accountability* ») du RGPD. Rendue obligatoire, elle permet au responsable de traitement ou au sous-traitant de garantir et de démontrer le respect de ses obligations ainsi que les démarches entreprises.

De nombreux éléments peuvent être intégrés dans la documentation, tels que le registre des activités de traitement, les AIPD, le registre des violations de données et des mesures prises pour y remédier, les mentions d'informations, les preuves du recueil du consentement, les procédures relatives à l'exercice des droits, les contrats de sous-traitance, les outils d'encadrement des transferts hors Union européenne, l'analyse écrite sur l'absence de conflit d'intérêts du DPO, etc. Cette liste n'est pas limitative dans la mesure où tout élément permettant de justifier de la conformité et de piloter les actions à réaliser peut être intégré à la documentation.

La documentation est un outil essentiel du DPO car elle permet d'avoir une connaissance exhaustive des opérations de traitement mises en œuvre et de prévoir leur pilotage. Le DPO doit donc s'assurer de la tenue de cette documentation, c'est-à-dire d'en garantir la pertinence et d'en piloter l'actualisation.

S'agissant de la **tenue du registre des activités de traitement**, l'article 30 du RGPD prévoit que l'obligation de tenir un registre pèse sur le responsable du traitement ou le sous-traitant. Or, dans la pratique, les activités du DPO peuvent le conduire à prendre en charge cette mission. En effet, la tenue du registre constitue un outil de suivi et de contrôle des traitements mis en œuvre permettant au DPO d'avoir une connaissance la plus exhaustive possible des opérations de traitements et de proposer les mesures nécessaires à leur encadrement. Il doit en tout état de cause pouvoir le consulter à tout moment.

À noter : il est recommandé de prévoir dans la lettre de mission du DPO que la tenue du registre constitue l'une de ses missions (si c'est effectivement le cas) et d'indiquer que les informations relatives à chaque traitement lui seront communiquées par les personnes qui en ont la charge ou qui les mettent en œuvre.

Pour plus d'information sur le registre des traitements, la CNIL a publié une fiche dédiée sur son site web, qui contient notamment un modèle de registre simplifié, en tableur, au format ouvert, librement réutilisable et qui peut s'adapter à de nombreux cas de traitements de données, ainsi que le registre de la CNIL.

Questions fréquentes

Comment le DPO doit-il prioriser ses missions ?

Si l'ensemble des missions présentées ci-dessus doit être mis en œuvre par le DPO, le RGPD précise que le DPO « 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 » (article 39.2). Cela signifie que le niveau de vigilance et de moyens doit être d'autant plus fort que les risques présentés par les traitements sont importants (suivi rigoureux des traitements de données sensibles, formation de collaborateurs particulièrement impliqués, audit interne sur les mesures de sécurité, etc.).

Le DPO doit-il lui-même répondre à toutes les demandes extérieures ?

Si la CNIL et toute personne concernée doivent pouvoir s'adresser au DPO dans les cas prévus par les textes, celui-ci n'est pas tenu d'être systématiquement à l'origine de la réponse. Il doit en revanche s'assurer que chaque demande recevra un traitement adapté par le service compétent dans les délais impartis.

Le DPO est-il responsable de la conformité ? Ses recommandations sont-elles obligatoires ?

Le DPO n'est pas personnellement responsable en cas de manquement aux obligations prévues par le RGPD. C'est l'organisme qui est responsable du respect du RGPD (voir la fiche n°6 sur le statut du DPO). Il est impossible de transférer au délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant.

Si les recommandations du DPO ne sont pas suivies, le responsable de traitement ou le DPO peuvent utilement documenter les décisions qui ont été prises ainsi que, le cas échéant, les raisons pour lesquelles l'avis du DPO n'a pas été suivi.

Le DPO peut-il effectuer d'autres missions que celles prévues à l'article 39 du RGPD ?

Il est tout à fait possible de confier au DPO d'autres tâches à la condition que cela ne fasse pas obstacle à la réalisation des missions qui lui sont spécifiquement attribuées par le RGPD (y compris en le privant du temps nécessaire à l'exécution de ces missions) et ne constitue pas un conflit d'intérêts.

Certaines tâches apparaissent adaptées, par nature, à la fonction du DPO et pourraient lui être utilement attribuées, comme la tenue du registre des activités de traitements, la participation à la réalisation ou à l'évaluation des analyses d'impact, s'il en a les compétences, ou la supervision des cas de violation de données personnelles.

Il convient de noter qu'aucune de ces missions ne peut être effectuée solitairement par le DPO qui doit nécessairement pouvoir travailler avec les équipes traitant ou déterminant les traitements de données personnelles. Par ailleurs, ces obligations demeurent de la responsabilité du responsable de traitement ou du sous-traitant.

TEXTES OFFICIELS

Sur cnil.fr :
- Articles 38 et 39 du RGPD sur la fonction et les missions du DPO.
- Articles 82 et suivants du décret d'application de la loi Informatique et Libertés, légifrance.fr.
- La « Charte des contrôles » de la CNIL.

LA DÉSIGNATION DU DPO

Fiche 1 : Dans quels cas faut-il désigner un DPO ?

Qu'ils soient responsables de traitement ou sous-traitants, la désignation d'un délégué est **obligatoire** pour :

- les autorités ou organismes publics (à l'exception des juridictions dans l'exercice de leurs fonctions juridictionnelles) ;
- les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique de personnes à grande échelle ;
- les organismes dont les activités de base les amènent à traiter à grande échelle des données sensibles ou relatives à des condamnations pénales et infractions.

BONNE PRATIQUE

Même en dehors de ces trois cas, **la désignation d'un DPO est recommandée dès que l'organisme rencontre des problématiques relatives à la protection des données personnelles**. Cela permet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données.

Que regroupe l'appellation « autorités et organismes publics » ?

Il s'agit des autorités nationales, régionales et locales mais également d'organismes tels que les structures de l'enseignement supérieur, hôpitaux, agences sanitaires, autorités administratives indépendantes (AAI), établissements publics à caractère administratif (EPA), etc.

BONNE PRATIQUE

Les organismes privés chargés d'une mission de service public conservent leur statut de droit privé et ne sont donc pas tenus de désigner un DPO. Néanmoins, comme souligné dans les lignes directrices sur le DPO du CEDP, **la désignation d'un délégué est encouragée pour ces organismes**, même dans les cas où elle ne serait pas obligatoire en vertu des autres critères.

« Activité de base » : de quoi s'agit-il ?

L'activité de base d'un organisme correspond à son cœur de métier. Si un traitement de données personnelles est essentiel pour atteindre les objectifs de l'organisme, alors ce critère est rempli.

Exemple : l'activité de base d'une clinique est de fournir des soins aux patients qu'elle prend en charge. Cette activité implique nécessairement des traitements de données relatives à la santé (dossiers médicaux des patients). Le traitement de ces données doit, dans ce cas, être considéré comme une activité de base de la clinique.

Cependant, l'activité en support ou « auxiliaire » (exemple : rémunération des employés, assistance informatique) ne constitue pas une activité de base de la clinique.

Comment évaluer le concept de « grande échelle » ?

Il s'agit des traitements qui visent à traiter « un volume considérable de données personnelles au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé » (considérant 91 du RGPD).

Il n'existe pas de seuil applicable à toute situation, à partir duquel un traitement est considéré comme mis en œuvre à « grande échelle ». Une analyse au cas par cas est nécessaire pour évaluer ce point. Cette analyse, et le raisonnement qui la sous-tend, peuvent utilement être intégrés à la documentation.

Elle doit prendre en compte un ensemble de facteurs :

- le nombre de personnes concernées, en valeur absolue ou en valeur relative (par rapport à la population concernée, et non pas par rapport à l'échelle de l'organisation) ;
- le volume de données et/ou le spectre des données traitées ;
- la durée ou la permanence des activités de traitement ;
- l'étendue géographique de l'activité de traitement.

EXEMPLES

Constituent des traitements à grande échelle :

- le traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités ;
- le traitement des données de voyage des passagers utilisant un moyen de transport public urbain (suivi par les titres de transport, par exemple) ;
- le traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans la fourniture de ces services ;
- le traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités ;
- le traitement des données personnelles par un moteur de recherche à des fins de publicité ciblée ;
- le traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet[1].

Ne constituent pas des traitements à grande échelle :

- le traitement des données de patients par un médecin de quartier exerçant à titre individuel si la patientèle est inférieure à 10 000 personnes par an (cf. le référentiel pour les cabinets médicaux et paramédicaux) ;
- le traitement des données personnelles relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

Qu'est-ce qu'un « suivi régulier et systématique » ?

Le RGPD ne définit pas la notion de « suivi régulier et systématique » des personnes, mais donne l'exemple de suivi et de profilage en ligne à des fins de publicité comportementale (considérant 24 du RGPD). Le CEPD indique qu'une ou plusieurs significations sont à envisager pour l'expression « régulier et systématique » :

- « régulier » doit s'entendre comme :
  - continu ou se produisant à intervalles réguliers au cours d'une période donnée ; ou
  - récurrent ou se répétant à des moments fixes ; ou
  - ayant lieu de manière constante ou périodique.
- « systématique » doit être compris comme :
  - se produisant conformément à un système ; ou
  - préétabli, organisé ou méthodique ; ou
  - ayant lieu dans le cadre d'un programme général de collecte de données ; ou
  - effectué dans le cadre d'une stratégie.

1 Tous ces exemples proviennent des Lignes directrices du CEPD sur le délégué à la protection des données

Exemples de suivi régulier et systématique des personnes concernées :

- activités de marketing dont la personnalisation est fondée sur les données personnelles ;
- profilage et notation à des fins d'évaluation des risques (évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent...) ;
- géolocalisation par des applications mobiles ;
- programmes de fidélité ;
- publicité comportementale ;
- surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables ;
- systèmes de télévision en circuit fermé ;
- dispositifs connectés tels que les voitures et compteurs intelligents, domotique, etc.

EXEMPLES DE DÉSIGNATION D'UN DPO

Partis politiques : les activités de base impliquent le traitement de catégories particulières de données (opinions politiques). Par conséquent, au vu de l'article 37.1.c du RGPD, le critère restant à évaluer pour déterminer si la désignation d'un DPO est obligatoire est le caractère « à grande échelle » du traitement.

Pour les partis politiques actifs au niveau national et ayant une base d'adhérents importante, le critère de grande échelle est vraisemblablement satisfait. En revanche, pour les petits partis ou les partis locaux, ce critère pourrait ne pas être rempli. Il convient de mener une analyse au cas par cas.

Commerçant ou grande distribution : la commercialisation des produits, l'encaissement des paiements et éventuellement la gestion des programmes de fidélité pourraient être considérés comme activités de base. Pour autant, ces activités peuvent ne pas exiger un suivi régulier et systématique des personnes concernées. Il convient donc de mener une analyse pour chaque traitement pour vérifier si cela est le cas, en particulier s'agissant de programmes de fidélité, et ainsi déterminer si la désignation du DPO est obligatoire.

POUR ALLER PLUS LOIN

Sur cnil.fr :
- Article 37.1 du RGPD sur les cas de désignations obligatoires du DPO.
- Considérant 97 du RGPD sur la notion d'activité de base.
- Considérant 31 du RGPD sur la notion de grande échelle.
- Considérant 24 du RGPD sur la notion de suivi du comportement des personnes.
- Lignes directrices du CEPD sur le délégué à la protection des données (p. 6 et suivantes).

Fiche 2 : Qui peut être désigné DPO ?

Bien qu'il n'existe **pas de profil type** pour exercer la fonction de DPO, le RGPD impose que le délégué dispose d'un certain niveau d'expertise. L'organisme doit également veiller à l'absence de conflit d'intérêts avec d'autres missions.

Connaissances et compétences du délégué

La personne pressentie à la fonction de DPO doit disposer d'un certain **niveau de connaissances**, c'est-à-dire :

- une expertise juridique et technique en matière de protection des données ;
- une connaissance du secteur d'activité, de la réglementation sectorielle et de l'organisation de la structure pour laquelle il est désigné ;
- une compréhension des opérations de traitement, des systèmes d'information et des besoins de l'organisme en matière de protection et de sécurité des données ;
- pour une autorité publique ou un organisme public, une bonne connaissance des règles et procédures administratives applicables.

Si la personne pressentie ne possède pas l'expertise sur toutes ces connaissances avant son entrée en fonction, il faudra nécessairement mobiliser l'expertise interne et développer à très court terme ses connaissances par des formations.

La personne doit également présenter les qualités personnelles nécessaires à cette fonction : intégrité, haut niveau d'éthique professionnelle, capacité à communiquer, vulgariser et convaincre.

À noter : le niveau d'expertise exigé varie en fonction de la sensibilité, de la complexité et du volume de données traitées par l'organisme. Ces connaissances et compétences peuvent être acquises au moyen d'un plan de formation adapté au profil du futur délégué (voir la question « Comment un DPO peut-il se former ? »).

FOCUS : LA CERTIFICATION DU DPO

La certification est la procédure par laquelle un tiers atteste de la conformité d'un produit, d'un service ou d'une compétence à une norme ou à un référentiel.

Depuis 2018, la CNIL agrée des organismes qui délivrent une **certification des compétences du DPO** sur la base de son référentiel, et tient une liste de ces organismes. Ceux-ci proposent un examen, sous la forme d'un questionnaire à choix multiples d'au moins cent questions portant sur la réglementation, la responsabilité et la sécurité.

Cette certification n'est accessible qu'après 2 ans d'expérience professionnelle en lien avec la protection des données, ou 2 ans en tout domaine et une formation sur le sujet d'au moins 35 heures. Elle est ensuite valable 3 ans.

Pour son titulaire, la certification constitue une preuve de son adéquation avec le niveau d'exigence de connaissance imposé par le RGPD. Pour les organismes à la recherche de profils d'experts « protection des données », la certification représente un gage de confiance. **Néanmoins, il n'est pas obligatoire d'être certifié pour être désigné DPO.**

Absence de conflit d'intérêts

Le DPO peut exercer d'autres fonctions au sein de l'organisme (DPO à temps partiel). Toutefois, dans le cadre de ses autres fonctions, il ne doit pas avoir de **pouvoir décisionnel sur la détermination des finalités et moyens de traitements** : le DPO ne doit donc pas être « juge et partie ».

L'existence d'un conflit d'intérêts s'apprécie **au cas par cas**. Il est conseillé de documenter l'analyse conduisant à exclure l'existence de conflit d'intérêts pour le DPO désigné.

Exemples de fonctions susceptibles de provoquer un conflit d'intérêts : directeur général des services, directeur des opérations, médecin-chef, responsable du département marketing, responsable des ressources humaines, responsable du service informatique, etc.

ATTENTION

Des fonctions de niveau hiérarchique « inférieur » au sein de la structure organisationnelle sont également susceptibles de donner lieu à un conflit d'intérêts **dès lors qu'en pratique la personne participe à la détermination des finalités et des moyens du traitement**.

FOCUS : DOCUMENTER LE CHOIX DE SON DPO

Lorsqu'un organisme désigne un DPO, il doit être en capacité de prouver que son **DPO répond aux exigences du RGPD** (connaissances et compétences, absence de conflit d'intérêts, etc.).

La CNIL ne vérifie pas ces prérequis au moment de la désignation. Selon le principe d'*accountability*, c'est à l'organisme qui désigne un DPO d'assembler en interne une documentation permettant d'attester que le délégué désigné répond aux exigences du RGPD. En cas de contrôle de la CNIL, il peut être demandé à l'organisme de présenter cette documentation.

Exemples : CV, fiche de poste, analyse écrite sur l'absence de conflit d'intérêts, éventuelle certification, etc.

Questions fréquentes

Quel profil faut-il posséder pour être DPO ?

Il n'existe pas de profil type du DPO. En effet, selon l'étude sur les DPO réalisée par l'AFPA en partenariat avec la CNIL[2], environ 28 % des DPO ont un profil informatique, et le même pourcentage un profil juridique, les 43 % restant provenant de l'administratif, de la finance, de la conformité, de l'audit, etc.

Un DPO doit-il justifier d'un diplôme particulier ?

L'obtention d'un diplôme particulier ou le suivi d'une formation spécifique ne sont pas exigés pour être désigné DPO. Cependant, le délégué doit disposer des compétences et connaissances adéquates pour exercer ses missions.

Ainsi, si le DPO ne dispose pas d'un diplôme spécialisé dans la protection des données, il aura fréquemment complété sa formation académique par une expérience professionnelle ou une formation continue dans la sécurité informatique, le droit, ou toute autre matière pertinente pour l'exercice de ses fonctions.

Le responsable de traitement recrutant un DPO doit s'assurer que le candidat retenu dispose des connaissances spécialisées requises et doit lui permettre d'entretenir et compléter ses savoirs.

DPO et RSSI : un conflit d'intérêts ?

Un responsable de la sécurité des systèmes d'information peut être désigné DPO s'il ne dispose pas, en tant que RSSI, d'un pouvoir décisionnel dans la détermination des finalités et des moyens des traitements de données personnelles mis en œuvre par sa structure.

DPO et représentant du personnel : un conflit d'intérêts ?

Un délégué du personnel peut être amené, dans le cadre d'un vote, à prendre position sur certains sujets ou projets en lien avec le traitement de données personnelles, notamment la gestion du personnel. Dans cette hypothèse, il peut exister un risque de conflit d'intérêts avec la fonction de DPO. Selon le même raisonnement, un DPO peut figurer dans un comité d'éthique ou de déontologie si tant est que cela ne crée pas de risques de conflits d'intérêts.

2 « Délégué à la protection des données (DPO) : un métier qui se développe, une fonction qui se structure », Étude réalisée par la direction prospective métier de l'AFPA, à la demande du ministère du Travail, de l'Emploi et de l'Inclusion (DGEFP), en partenariat avec la CNIL et l'AFCDP (2020).

Le représentant dans l'Union européenne d'un responsable de traitement ou d'un sous-traitant établi hors de l'Union peut-il être désigné DPO ?

Le représentant d'un responsable du traitement ou d'un sous-traitant qui n'est pas établi dans l'Union ne peut en principe pas être désigné DPO pour cet organisme car cela constituerait un conflit d'intérêts.

Une personne morale peut-elle être sous-traitante et DPO pour un même organisme ?

Il n'existe pas d'interdiction de principe à ce qu'un prestataire, par ailleurs sous-traitant[3], soit désigné DPO pour son client. Il s'agirait alors d'une prestation de services distincte qui ne s'effectuerait pas dans le cadre des instructions du responsable de traitement. Cela pourrait être le cas, par exemple, d'un organisme offrant des prestations de services numériques et de DPO externalisé.

Cependant, une **analyse au cas par cas** doit être menée pour évaluer si la situation est de nature à compromettre l'indépendance du DPO dans l'exercice de ses missions. Cette analyse participe de la documentation du responsable de traitement et du sous-traitant.

Dans certains cas, il est nécessaire de mettre en place des mesures permettant de garantir cette indépendance. Il convient alors de prêter attention :

- au statut (public ou privé) des acteurs en question, les acteurs publics n'étant pas soumis aux mêmes contraintes de profit ;
- à la possibilité de prévoir des points de contact différents chez le prestataire (un en tant que sous-traitant, un en tant que prestataire/DPO).
- à la possibilité de prévoir deux contrats distincts.

Pour ne pas se retrouver à la fois juge et partie, et être ainsi à l'abri des conflits d'intérêts, la personne exerçant la fonction de délégué ne doit toutefois avoir ni la position de dirigeant ni la qualité de donneur d'ordre au sein de la structure.

Une même personne peut-elle être DPO pour un responsable de traitement et son sous-traitant ?

Le RGPD n'interdit pas à un DPO d'être désigné pour un responsable de traitement et son sous-traitant.

Cependant, selon un raisonnement similaire à celui présenté ci-dessus et compte tenu de l'exigence d'indépendance, il est recommandé d'évaluer si l'organisation et les mesures prises permettent de garantir cette indépendance. Ces éléments devront être inclus dans la documentation du responsable de traitement et de son sous-traitant.

Il convient en particulier de définir comment cette indépendance peut être assurée dans les moments où les deux structures peuvent disposer d'intérêts divergents, par exemple dans le cadre de l'examen du contrat entre le responsable de traitement et le sous-traitant.

3 Un sous-traitant traite les données pour le compte, sur instruction et sous l'autorité d'un responsable de traitement (ex : hébergement, maintenance, etc.). .

Un même délégué peut-il être désigné pour des organismes concurrents ?

Un délégué externe peut être désigné pour des organismes en situation de concurrence, dès lors que ces différentes missions et tâches n'entraînent pas de conflits d'intérêts. En effet, le DPO est soumis à une obligation de confidentialité ou au secret professionnel et peut ainsi travailler pour des employeurs concurrents sans mettre en danger la confidentialité de chacune des parties.

Peut-on designer un avocat comme DPO ?

Un avocat peut être désigné DPO d'un organisme sur la base d'un contrat de service (DPO externe). Cependant, cet avocat ne peut pas représenter cet organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données personnelles dès lors que cette représentation pourrait constituer un conflit d'intérêts.

Un élu politique peut-il être DPO ?

Un élu ne peut pas exercer les fonctions de délégué pour la collectivité dont il est élu en raison d'un conflit d'intérêts. En effet, ce dernier participe à la prise des décisions sur les traitements de données mis en œuvre par la collectivité.

Un secrétaire de mairie peut-il être DPO ?

Dans les petites collectivités, les secrétaires de mairie sont souvent pressentis pour occuper la fonction de DPO. Or, l'exercice des missions associées peut parfois se heurter à des difficultés : manque de temps à consacrer au sujet et risque de conflits d'intérêts.

Ainsi, avant de procéder à la désignation, le maire doit bien s'assurer que le DPO pressenti ne prend pas part aux décisions concernant les fichiers exploités par la collectivité (objectifs et conditions de mise en œuvre, données traitées, destinataires, durées de conservation, mesures de sécurité, etc.) et qu'il dispose du temps suffisant pour accomplir ses missions.

Un stagiaire ou un apprenti peut-il être DPO ?

Bien que cette possibilité ne soit pas exclue explicitement par le RGPD, elle apparaît difficilement compatible avec les exigences liées à l'exercice de la fonction. Outre les difficultés que cette désignation pourrait comporter en termes de droit du travail (affectation d'un stagiaire à un poste de travail permanent), il faut relever que :

- le DPO doit disposer de « connaissances spécialisées » alors que le stagiaire/apprenti est en poste pour apprendre ;
- le stagiaire/apprenti devrait pouvoir bénéficier de conseils et de remarques sur son travail, ce qui contredit le fait que le DPO ne doit recevoir aucune instruction sur l'exercice de ces missions ;
- la mission du DPO est une mission au long cours, aussi bien dans la mise en conformité initiale de l'organisme que dans le suivi des nouveaux projets, ce qui se concilie mal avec la durée limitée d'un stage. À ce titre, les lignes directrices du CEPD sur le DPO recommande de privilégier les contrats les plus longs pour ce poste.

Comment évaluer l'indépendance du DPO ?

L'indépendance réelle du DPO, dans son rôle d'analyse et de conseil, suppose que deux types d'impartialités soient respectés :

- une impartialité objective : le DPO n'est pas juge et partie, car il n'est pas amené à contrôler ce qu'il a lui-même décidé, seul ou conjointement ;
- une impartialité subjective : le DPO est à l'abri d'influences guidées par des intérêts divergents, de nature à altérer la liberté de ses positionnements.

Que risque un organisme qui ne désigne pas de DPO ?

Un organisme qui n'aurait pas désigné de DPO lorsque cette désignation est obligatoire s'exposerait à une sanction de la CNIL, qui pourrait notamment prendre la forme d'un rappel à l'ordre, d'une injonction à se mettre en conformité ou d'une amende administrative pouvant s'élever jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

TEXTES OFFICIELS

Sur cnil.fr :
- Article 37.5 du RGPD sur les connaissances et compétences du délégué.
- Article 38.6 du RGPD sur l'absence de conflit d'intérêts.
- Lignes directrices du CEPD relatives au délégué à la protection des données (p.13 et suivantes ; p. 19 et suivantes).

Fiche 3 : DPO interne ou externe ? Comment mutualiser la fonction ?

Chaque organisme est libre d'organiser la fonction de DPO selon ses besoins. Il s'agit d'un choix qui appartient à l'entité, en fonction notamment des avantages et inconvénients du recours à un DPO externe ou interne, de l'offre interne disponible et de l'organisation de la structure.

DPO interne

Le délégué peut être un membre du personnel de l'organisme. Il peut exercer ses fonctions à temps plein ou à temps partiel.

Avantages :

- connaissance de l'organisation de la structure, des services ainsi que du secteur d'activité ;
- proximité avec les interlocuteurs internes ;
- meilleure réactivité en cas de sollicitation interne sur les sujets en lien avec la protection des données ;
- plus facile de prévoir sa présence en cas de contrôle de la CNIL.

Points de vigilance :

- risque de conflit d'intérêts si le délégué exerce d'autres missions ;
- attribution de temps suffisant au délégué ;
- positionnement hiérarchique adéquat ;
- éventuel plan de formation adapté au profil du DPO à prévoir.

DPO externe

La fonction de DPO peut être exercée sur la base d'un contrat de service conclu avec une personne physique (exemple : consultant, salarié d'une filiale du groupe, etc.) ou morale (exemple : cabinet d'avocats, cabinet de conseil, centre de gestion, syndicat mixte, etc.).

Avantages :

- solution à l'absence de ressources humaines internes ;
- recours à l'expérience et aux outils développés par le délégué externe ;
- spécialisation du DPO dans un secteur ;
- connaissance des bonnes pratiques pour des organismes similaires.

Points de vigilance :

- organisation de points d'échange et de contacts réguliers avec le niveau le plus élevé de la direction, ainsi qu'avec les équipes métiers pour maintenir une proximité ;
- rendre le contact du DPO externe aussi systématique, simple et facile que le contact d'une personne interne ;
- difficulté de choisir son prestataire et de s'assurer de son expertise

DPO mutualisé

Qu'il s'agisse d'un délégué interne ou externe, un DPO peut être mutualisé, c'est-à-dire désigné pour plusieurs entités.

Avantages :

- lissage des coûts liés à la désignation du délégué pour les entités d'un même groupe ;
- uniformisation des procédures entre les entités ayant mutualisé la fonction ;
- pilotage transversal de la conformité entre organismes ayant les mêmes préoccupations.

Points de vigilance :

- organisation des points d'échange et de contacts réguliers avec les équipes métiers pour maintenir une proximité ;
- risque pour le délégué de ne pas être tenu informé des sujets internes liés à la protection des données ;
- mise en place d'une organisation permettant d'assurer un pilotage efficient de la conformité (ex : relais, référents).

La mutualisation est possible sous **certaines conditions** qui varient selon le type de structure :

- **pour le secteur privé :** un groupe d'entreprises peut désigner un seul DPO à condition qu'il soit **facilement joignable à partir de chaque lieu d'établissement**.

EXEMPLES

Dans le cas d'un groupe composé de 6 filiales implantées dans différents États membres de l'Union européenne, un seul délégué (salarié d'une des filiales ou prestataire externe) peut être désigné pour la maison mère et l'ensemble des sociétés du groupe à condition de mettre en place une organisation adéquate.

N'étant pas physiquement présent dans chacune des filiales, le délégué peut, par exemple, être soutenu par un réseau de « relais » ou de « référents » chargés notamment d'apporter un appui opérationnel au DPO, tout en lui faisant remonter les questions qui se posent.

- **pour le secteur public :** la fonction de délégué peut être mutualisée entre plusieurs autorités ou organismes publics, **compte tenu de leur structure organisationnelle et de leur taille**.

La mutualisation est une solution particulièrement adaptée pour **les plus petites collectivités territoriales**. Elle leur permet en effet de diminuer les coûts financiers associés à la fonction, tout en bénéficiant des services de professionnels disposant de compétences Informatique et Libertés, de la connaissance des problématiques propres au secteur public local et de la disponibilité nécessaire à un exercice efficace des missions.

Elle peut, notamment, intervenir au niveau d'un établissement public de coopération intercommunale, telle une communauté de communes ou d'agglomération, ou d'un opérateur public de services numériques, comme un syndicat mixte, une agence technique départementale ou un centre de gestion de la fonction publique territoriale accompagnant le développement de l'e-administration sur son territoire.

Les collectivités territoriales, établissements publics locaux et organismes privés chargés d'une mission de service public qui optent pour la mutualisation doivent conclure une convention définissant les conditions dans lesquelles celle-ci s'exerce.

Pour plus d'information sur les initiatives de mutualisation au sein des collectivités territoriales

Voir les fiches « En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ? » et « Désigner un délégué à la protection des données dans une collectivité » sur le site web de la CNIL (rubrique « Collectivités territoriales »).

FOCUS : LA CONVENTION DE MUTUALISATION POUR LES ORGANISMES PUBLICS

Les collectivités territoriales, les établissements publics administratifs locaux, et les personnes morales de droit privé gérant un service public qui optent pour la mutualisation ont l'obligation de conclure une **convention de mutualisation** (art. 84 du décret d'application de la loi Informatique et Libertés).

Cette convention définit les conditions dans lesquelles s'exerce cette mutualisation.

4 « Délégué à la protection des données (DPO) : un métier qui se développe, une fonction qui se structure », Étude réalisée par la direction prospective métier de l'AFPA, à la demande du ministère du Travail, de l'Emploi et de l'Inclusion (DGEFP), en partenariat avec la CNIL et l'AFCDP (2020).

Questions fréquentes

DPO interne : temps partiel ou temps plein ?

Il s'agit d'une décision laissée à l'appréciation du responsable de traitement ou du sous-traitant qui désigne un DPO.

La désignation d'un délégué à temps partiel impose une évaluation de sa charge de travail afin de lui allouer le temps nécessaire à l'exercice de ses missions (voir fiche n°5).

Selon l'étude réalisée par l'AFPA en partenariat avec la CNIL[4], seul un quart des DPO internes exerce cette mission à temps plein.

Un DPO peut-il être désigné pour une durée limitée ?

Les organismes pour lesquels la désignation d'un délégué n'est pas obligatoire peuvent prévoir que le DPO, interne ou externe, exerce ses missions pour une durée limitée. Celle-ci doit cependant être suffisante pour lui permettre un travail approfondi sur la mise en conformité qui, dans une large majorité des cas, requiert plusieurs mois voire plusieurs années. Une disponibilité temporelle de long terme peut faire partie des moyens que l'organisme fournit au DPO. Il est conseillé de formaliser ce point dans la lettre de mission ou dans le contrat de prestation de service.

DPO externe : quelles sont les exigences vis-à-vis des salariés de l'organisme désigné DPO ?

Lorsque la fonction de délégué est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut, dans les faits, exercer les missions du délégué en tant que groupe. Dans ce cas, il est conseillé de prévoir, dans le contrat de service, une répartition claire des tâches au sein de l'équipe externe chargée de la fonction de DPO et d'identifier clairement la personne qui agit comme le contact en charge du client.
Il est également recommandé que chaque collaborateur du prestataire exerçant les fonctions de DPO remplisse l'ensemble des exigences applicables (indépendance, ressources et moyens suffisants, absence de conflit d'intérêts, etc.).

DPO mutualisé : comment désigner auprès de la CNIL ?

En cas de mutualisation de la fonction de DPO pour un groupe d'entités, chacune de ces entités doit, en tant que responsable de traitement ou sous-traitant, compléter un formulaire de désignation du délégué.

Pour les entités ayant un nombre important de désignations à réaliser, une procédure de désignation spécifique (« désignation multiple ») est proposée (pour plus d'information, contactez le service des DPO de la CNIL).

TEXTES DE RÉFÉRENCE

Sur cnil.fr :
- Article 37.6 du RGPD sur la désignation d'un délégué interne ou externe.
- Articles 83 et 84 du décret n° 2019-536 du 29 mai 2019 sur les modalités de désignation du DPO auprès de la CNIL et la convention de mutualisation professionnelle.

LA DÉSIGNATION DU DPO

Fiche 4 : comment désigner un DPO ?

Étape n° 1 : choisir le « bon DPO »

Un DPO externe peut être une personne physique ou morale, mais un DPO désigné en interne ne peut être qu'une personne physique (un salarié, par exemple).
La procédure de désignation interne d'un DPO impose de s'interroger préalablement sur la personne pressentie pour ce poste : il est à cet égard important de se poser les bonnes questions afin, par la suite, d'être en capacité de justifier son choix.

Le choix d'un DPO en interne doit notamment tenir compte de :

- l'intérêt de la personne pressentie pour les missions du DPO et l'appétence pour la matière de la protection des données ;
- son profil au regard de ses qualifications et de son absence de conflits d'intérêts (voir fiche n° 2) ;
- les conditions d'exercice de ses missions (ressources suffisantes, accès aux informations utiles et indépendance - voir fiches n°5 et 6).

DÉSIGNER UN DPO : LES QUESTIONS CLÉS

Le document « Les questions clés à se poser lors de la désignation d'un DPO » (annexe n° 1) permet de vérifier que les exigences du RGPD concernant un futur délégué sont satisfaites.

Étape n° 2 : formaliser la désignation

Il est recommandé de formaliser les missions confiées au DPO au travers d'un document spécifique. Exemples : lettre de mission, avenant au contrat de travail, fiche de poste, contrat de prestation de service pour le DPO externe, etc.

Ce document peut également être l'occasion de définir les modalités de travail du DPO (moyens alloués, interlocuteurs relais identifiés, fréquence des réunions avec la direction de l'organisme et les services traitant les données, circuit de communication, etc.) en décrivant comment les obligations de l'organisme désignant seront transposées en pratique.

EXEMPLE DE LETTRE DE MISSION

Le présent guide propose un exemple de lettre de mission à remettre au DPO (voir Annexe n° 2). Cette dernière doit bien sûr être adaptée et précisée en fonction des missions dévolues au délégué et des conditions d'exercice de sa fonction.

Étape n° 3 : faire connaître son DPO

La désignation d'un DPO devrait s'accompagner **d'actions de communication** à même d'apporter de la visibilité à la fonction et aux coordonnées du délégué au sein de l'organisme, par exemple vis-à-vis de tous les collaborateurs (agents ou salariés), des instances représentatives du personnel et des comités de direction ou instances exécutives.
Exemples d'actions de communication : note d'information envoyée par la direction à l'ensemble du personnel, note interne publiée sur l'intranet ou par affichage (voir, à titre d'exemple, l'affiche de la CNIL « Adoptez les 6 bons réflexes ») , présentation interne devant les instances de direction, publication de la lettre de mission, etc.

Ce type d'actions a pour objectif de communiquer en interne sur le rôle du DPO, son statut, les moyens qui lui sont affectés et les procédures associées à l'exercice de ses missions. C'est aussi l'occasion de rappeler l'enjeu de la conformité et de présenter les futurs chantiers qui seront pilotés par le DPO.

À noter : le délégué est en contact permanent avec les services et directions de l'organisme. Ce plan de communication est donc particulièrement important dans la mesure où il assure au DPO les conditions les plus favorables à sa prise de fonction.

Étape n° 4 : désigner son DPO auprès de l'autorité de contrôle compétente

Avant de procéder à la désignation de son délégué, un organisme travaillant dans plusieurs pays doit s'assurer que la CNIL est l'autorité compétente pour la désignation (voir la question « Auprès de quelle autorité de contrôle désigner mon DPO ? »). S'il s'agit de la CNIL, il peut alors procéder à la désignation en ligne de son délégué.

La désignation du DPO auprès de la CNIL ne se fait qu'en ligne via le téléservice dédié. Aucun courrier postal n'est traité et il n'est pas nécessaire d'envoyer de documents justificatifs tels qu'une délibération du conseil municipal portant désignation du délégué.

Les 4 étapes du formulaire de désignation sont détaillées dans l'annexe 3 de ce guide.

Questions fréquentes

Un DPO peut-il faire l'objet d'une désignation partielle ?

Le DPO est désigné pour toutes les opérations de traitement effectuées par le responsable du traitement ou le sous-traitant (point 2.1 des lignes directrices du CEPD sur le DPO). Par conséquent, la désignation partielle d'un DPO (exemple : désignation d'un DPO uniquement pour les traitements RH) n'est pas possible.

Le rôle de DPO peut-il être rempli par plusieurs personnes ?

Un organisme ne peut désigner qu'une seule personne en tant que délégué à la protection des données. Celui-ci peut cependant être épaulé par une équipe, travailler en collaboration avec les autres métiers de l'organisme ou disposer d'un réseau de « relais Informatique et Libertés » à même de l'aider à sensibiliser aux questions de protection des données ou de lui faire remonter les questions, les projets ou les demandes d'exercice de droit.

Les instances représentatives du personnel doivent-elles obligatoirement être informées de la désignation du DPO ?

L'information des instances représentatives du personnel n'est pas exigée par la réglementation. Cela reste toutefois une bonne pratique afin d'assurer une transparence et une bonne visibilité de la désignation du délégué au sein de l'organisme.

Collectivités territoriales : la désignation du DPO nécessite-t-elle l'envoi à la CNIL d'une délibération ou d'un arrêté se rapportant à l'exercice de la fonction ?

Non, aucun document justificatif n'est demandé pour la désignation du délégué auprès de la CNIL. Pour les collectivités territoriales, il n'est donc pas nécessaire de lui envoyer, en complément du suivi de la procédure en ligne prévue à cet effet, l'éventuelle délibération portant création de l'emploi ou l'arrêté portant désignation du délégué. Seule la procédure en ligne est nécessaire pour désigner un DPO.

À quelle date la désignation du délégué devient-elle effective ?

La désignation du délégué est effective le lendemain de la validation du formulaire de désignation en ligne par l'organisme.

Auprès de quelle autorité de contrôle en Europe désigner mon DPO ?

La détermination de l'autorité auprès de laquelle il convient de désigner le DPO ne dépend ni de la localisation de celui-ci, ni de la qualité de société-mère ou de filiale de l'organisme. En revanche, la nature des traitements mis en œuvre a une incidence :

- **Pour les traitements locaux** (mis en œuvre par les établissements d'un organisme dans un seul pays et n'affectant sensiblement que des personnes de ce pays) : le DPO doit être désigné auprès de **l'autorité locale compétente** s'agissant des traitements locaux (siège social du responsable de traitement ou du sous-traitant, qui correspond à l'autorité de l'État membre où sont mis en œuvre les traitements locaux).
- **Pour les traitements transfrontaliers :** dans l'hypothèse où le responsable de traitement (mère ou filiale) met également en œuvre des traitements transfrontaliers, le DPO doit être désigné auprès de **l'autorité chef de file**.

L'autorité chef de file est celle du pays où est situé l'établissement principal (lieu du siège social ou lieu de l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement). Par conséquent, elle est fréquemment également compétente pour certains traitements locaux.

EXEMPLE

Un DPO est mutualisé pour un groupe de sociétés dont la maison mère est en Italie et la filiale en France. En tant que DPO de la filiale française, il doit être désigné auprès de la CNIL s'agissant des traitements locaux et des traitements transfrontaliers dont la filiale française est responsable de traitement. Aucune démarche auprès de l'autorité italienne n'est requise par la filiale française. De la même façon, la maison mère en Italie doit désigner ce DPO auprès de l'autorité de contrôle italienne pour ses traitements locaux et les traitements transfrontaliers dont elle est responsable de traitement.

Ce raisonnement s'applique qu'il s'agisse du même DPO désigné pour l'ensemble des entités du groupe (mutualisé) ou d'un DPO différent pour chaque entité du groupe.

Est-il possible pour un salarié de refuser d'être désigné DPO ?

Les règles générales du droit du travail s'appliquent ici : si cette désignation constitue une modification substantielle du contrat de travail, alors la personne doit être mise en position de la refuser. À cette règle générale peuvent s'ajouter des règles particulières si, par exemple, la modification du contrat de travail était prévue dans le contrat ou si le salarié est par ailleurs un salarié protégé (représentant du personnel par exemple).

Les raisons amenant un salarié à refuser ou à souhaiter refuser la fonction de DPO (pas assez de ressources pour organiser la fonction, notamment temporelles, pas de connaissances suffisantes, etc.) peuvent être un **indice sérieux que les obligations incombant à l'organisme lors de la désignation du délégué ne sont pas respectée**s.

TEXTES DE RÉFÉRENCE

Sur cnil.fr :
- Article 37.7 du RGPD sur la désignation du DPO auprès de l'autorité de contrôle.
- Articles 83 et 84 du décret n° 2019-536 du 29 mai 2019 sur les modalités de désignation du DPO auprès de la CNIL et la convention de mutualisation.
- Lignes directrices du CEPD sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant.

L'EXERCICE DE LA FONCTION DE DPO

Fiche 5 : quels moyens doivent être attribués au DPO ?

Le délégué doit bénéficier des moyens nécessaires à l'exercice de ses missions, ce qui signifie qu'il doit être **associé à toutes les questions relatives à la protection des données et disposer de ressources suffisantes**.

L'association du DPO à toutes les questions relatives à la protection des données

Il est essentiel que le délégué ou, le cas échéant, son équipe, soit associé le plus tôt possible à toutes les questions relatives à la protection des données. L'information et la consultation du DPO dès qu'un projet de traitement est envisagé permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception (dite « by design »). **Le DPO doit être un interlocuteur naturel au sein de l'organisme**, par exemple en étant associé aux groupes de travail consacrés aux activités de traitement de données au sein de l'organisme.

À titre d'exemple, l'organisme veille notamment à ce que :

- le DPO soit invité à participer régulièrement aux réunions stratégiques de l'organisme qui définissent en amont les projets impliquant des données personnelles ;
- sa présence soit recommandée lorsque des décisions ayant des implications en matière de protection des données sont prises ;
- le DPO puisse dialoguer et travailler avec les fonctions jouant un rôle important dans la protection des données, telles que le responsable de la sécurité des systèmes d'information ;
- toutes les informations pertinentes soient transmises au DPO en temps utile afin de lui permettre de fournir un avis pertinent et éclairé ;
- l'avis du DPO soit toujours sérieusement pris en considération. En cas de désaccord, il est recommandé, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPO n'a pas été suivi ;
- le DPO soit immédiatement consulté lorsqu'une violation de données ou un autre incident (signalement relevé dans la presse, réclamations, etc.) se produit.

Les ressources du DPO

Le RGPD prévoit que l'organisme doit **fournir au DPO les ressources nécessaires à la réalisation de ses tâches** (temps nécessaire, accès à des ressources financières, collaborateurs s'il en a le besoin) ; en lui **facilitant l'accès aux données et aux opérations de traitement** (accès facilité aux autres services de l'organisme) et en lui **permettant d'entretenir ses connaissances spécialisées**.

Les ressources du DPO doivent être adaptées à la taille, la structure et l'activité de l'organisme. Ainsi, plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées au DPO devront être importantes.

Il est recommandé de préciser le type de ressources allouées au DPO dans la lettre de mission, en tant qu'engagement de l'organisme vis-à-vis du DPO pour lui permettre d'exercer au mieux ses missions.

EXEMPLES DE RESSOURCES À FOURNIR AU DPO

- La reconnaissance et la valorisation **de la fonction du DPO par l'encadrement supérieur** (par exemple, au niveau du conseil d'administration).
- Le **temps suffisant** pour que le DPO puisse accomplir ses tâches. Cet aspect est particulièrement important lorsque le DPO exerce ses missions à temps partiel. Il est également recommandé de déterminer, conjointement avec le DPO, l'estimation du temps nécessaire à l'exercice de sa fonction (le besoin est plus important lors de l'entrée dans la fonction), qu'un plan de travail soit défini et que les tâches du DPO y soient priorisées.
- Le soutien adéquat du point de vue des **ressources financières** (détenir un budget propre ou disponible pour des actions de sensibilisations ou pour recruter une équipe de façon temporaire ou permanente) et des **infrastructures** (locaux, installations, équipements).
- **L'accès par défaut à la documentation juridique** engageant l'organisme avec des tiers sur les questions de traitements de données personnelles (partenaires et sous-traitants).
- La **communication officielle de la désignation du DPO à l'ensemble du personnel** afin que l'existence et la fonction de celui-ci soient connues au sein de l'organisme.
- L'**accès aux outils de communication interne** dans l'accomplissement de ses missions afin de pouvoir sensibiliser et former aux exigences du RGPD (rappel des bonnes pratiques, réaction en cas d'emails frauduleux ou de violations de données, etc.).
- L'**accès à d'autres services**, tels que les ressources humaines, le service juridique, le service informatique, la sécurité, etc., de manière à ce que le DPO reçoive les contributions et les informations essentielles de ces autres services.
- La **formation continue**. Le DPO doit pouvoir maintenir ses connaissances à jour en ce qui concerne les évolutions réglementaires et techniques, notamment dans le domaine de la protection des données. Afin d'augmenter constamment le niveau d'expertise du DPO, ce dernier doit être encouragé à participer à des formations ainsi qu'à d'autres formes de développement professionnel, telles que la participation à des forums sur la protection de la vie privée, des ateliers, des associations professionnelles, etc.
- En fonction de la taille et de la structure de l'organisme, il pourrait être opportun de constituer une **équipe autour du DPO** dont les tâches et responsabilités de chacun des membres doivent être clairement établies. De même, lorsque la fonction du DPO est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut exercer les missions du DPO, sous la responsabilité d'une personne de contact principale désignée pour le client.

Questions fréquentes

Comment évaluer les ressources à allouer au DPO ?

La nature et le volume des ressources allouées au DPO varient selon la taille, la structure et l'activité de l'organisme. Dès lors, plus les opérations de traitement sont complexes ou susceptibles de porter atteinte à la vie privée des personnes, plus les ressources octroyées au DPO devront être importantes. Par exemple, l'analyse de projets complexes par le DPO nécessite du temps pour délivrer des conseils pertinents. L'estimation de la charge de travail doit être proportionnée aux priorités établies. Cette évaluation est essentielle au bon exercice des missions du DPO au profit de l'organisme qui le désigne.

La dotation d'un budget spécifique peut faire partie des moyens matériels à la disposition du délégué. Pour quantifier ce budget, différents éléments peuvent être pris en compte : par exemple, les besoins en termes de formation du futur DPO, les éventuelles actions de sensibilisation du personnel de l'organisme, le recours à des prestataires si nécessaire (avocats, auditeurs...) ou encore la contribution d'autres services au sein de l'organisme.

Les courriers adressés au DPO sont-ils confidentiels ?

Si le DPO peut souhaiter que son courrier soit ouvert à des fins de tri, il est également en droit de demander la mise en place d'un canal de communication strictement confidentiel (courriers inscrits « confidentiels » qui ne seront pas ouverts, emails chiffrés, ligne téléphonique confidentielle, etc.) en particulier à des fins de communication avec les personnes concernées en relation de subordination avec l'organisme.

Comment garantir l'accès du DPO aux données de l'organisme ?

Le DPO doit, en raison de ses missions, pouvoir accéder aux systèmes d'information de l'organisme, à la documentation contractuelle ainsi qu'aux informations traitées. Le responsable de traitement doit s'assurer que les services sous son autorité facilitent cet accès à la demande du délégué. En raison des enjeux en la matière, il est conseillé que le délégué et le responsable s'entendent sur un document formalisant les cas et les conditions dans lesquelles ces accès seront réalisés (exemple : . audit, vérification ponctuelle, instruction d'une demande de droits, violations de données, etc.).

Le DPO est soumis au secret professionnel ou à une obligation de confidentialité, et son accès aux données est soumis aux mêmes principes généraux que tous les salariés : il doit être proportionné, justifié et traçable.

Ces modalités pourront être prévues afin d'adapter au mieux les accès aux besoins du DPO (accès aux données en lecture / écriture, accès temporaire, possibilités d'extraction d'une base de données, etc.). Dans certains cas spécifiques sensibles (exemple : accès aux dossiers sur le poste d'un salarié, à des courriels, à des informations hautement confidentielles) des règles spécifiques pourront être prévues avec le DPO afin de garantir la réalisation de ses missions (exemple : vérifications opérées par un organisme tiers).

Cet accès doit comprendre les fichiers contenant des données personnelles ainsi que ceux supposés ne pas en contenir (les manquements au RGPD en matière de conservation et confidentialité sont régulièrement constatés par la CNIL au sein de fichiers que les organismes réputaient exempts de données personnelles).

L'organisme doit s'assurer que ces limites et accommodements n'empêchent pas la bonne réalisation des missions du DPO.

TEXTES OFFICIELS

Sur cnil.fr :
- Article 38.2 du RGPD sur l'obligation de fournir des ressources au DPO.
- Article 39.1 du RGPD sur les missions du DPO.
- Article 25 du RGPD sur la protection des données par défaut.
- Lignes directrices du CEPD relatives au délégué à la protection des données (p.16).

L'EXERCICE DE LA FONCTION DE DPO

Fiche 6 : Quel est le statut du DPO ?

L'indépendance du DPO dans l'exercice de ses missions

Le RGPD prévoit certaines garanties destinées à faire en sorte que le délégué soit en mesure d'exercer ses missions avec un degré suffisant d'autonomie et d'indépendance vis-à-vis de l'organisme qui le désigne.

Cette indépendance signifie que le DPO :

- **Ne doit pas recevoir d'instruction dans l'exercice de ses missions**, par exemple sur la manière de traiter un sujet, d'instruire une réclamation, sur le résultat à apporter à un audit interne ou encore sur l'opportunité de consulter l'autorité de contrôle. De même, il ne peut être tenu d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données telle qu'une interprétation particulière du droit.
- **Ne doit pas faire l'objet d'une sanction ou d'un licenciement du fait de l'accomplissement de ses missions**, par exemple si le délégué conseille au responsable de traitement d'effectuer une analyse d'impact et que celui-ci n'est pas d'accord, ou consigne une analyse juridique ou technique en contradiction avec celle retenue par le responsable de traitement. À noter toutefois qu'il peut être mis fin aux fonctions du délégué pour des raisons relevant de la législation du travail habituelle (tel que : vol, harcèlement, autre faute grave).
- **Fait directement rapport aux échelons les plus élevés de la direction de l'organisme** afin que le niveau auquel les décisions sont prises ait connaissance des avis et recommandations du DPO. Ainsi, la CNIL recommande que le délégué élabore et présente au niveau le plus élevé de l'organisme un rapport régulier (par exemple, annuel) sur ses activités. Le DPO doit également être en capacité de s'adresser directement au niveau le plus élevé sur une problématique spécifique s'il l'estime nécessaire[5]. À noter que cette exigence de faire rapport au niveau le plus élevé ne préjuge pas du « rattachement » du délégué pour lequel le RGPD ne comporte pas d'exigence.

Absence de responsabilité du DPO en cas de non-respect du RGPD

Le RGPD prévoit que c'est le responsable du traitement qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément au RGPD. De la même manière, c'est le sous-traitant qui est responsable du respect de ses obligations propres prévues par le RGPD. Dès lors, **le délégué n'est pas responsable en cas de non-respect du RGPD au sein de l'organisme qui l'a désigné**.

Il n'est donc pas possible de transférer au DPO, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant découlant du RGPD. En effet, cela reviendrait à conférer au DPO un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts contraire au RGPD.

5 À ce sujet, la Commission Nationale de la Protection des Données du Luxembourg a estimé dans sa décision n°23FR/2021 du 29 juin 2021 qu'un rattachement hiérarchique direct ou la possibilité de contourner les niveaux hiérarchiques intermédiaires pouvaient être des mesures proportionnées pour garantir l'autonomie du DPO.

Obligation de confidentialité/secret professionnel

Le délégué doit être soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions. Il convient donc de veiller à insérer une telle obligation dans le contrat de travail ou la lettre de mission du délégué interne ou dans le contrat de service du délégué externe.

À noter : cette obligation de secret professionnel ou de confidentialité n'interdit pas au DPO de prendre contact avec l'autorité de contrôle pour solliciter son avis. En effet, le RGPD prévoit que le DPO peut mener des consultations auprès de l'autorité de contrôle sur tout sujet.

Questions fréquentes

Le DPO peut-il être sanctionné pénalement dans l'exercice de ses missions?

Le DPO n'est pas pénalement responsable de la conformité de son organisme. Il peut, cependant, comme n'importe quel autre employé ou agent, voir sa responsabilité pénale engagée s'il enfreint intentionnellement les dispositions pénales de la loi Informatique et Libertés ou en tant que complice s'il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions pénales.

Le DPO peut-il être sanctionné civilement dans l'exercice de ses missions ?

L'hypothèse de la mise en jeu de la responsabilité civile du DPO pour l'exercice de ses missions ne peut pas concerner le DPO salarié : en application du principe de la responsabilité de l'employeur du fait de ses préposés, l'action civile initiée par une personne concernée par le traitement de données en cause ne pourrait être engagée que contre le responsable de traitement. En revanche, concernant le DPO externe, si ce dernier devait commettre une faute professionnelle conduisant le responsable de traitement à subir un préjudice, ce dernier pourrait rechercher la responsabilité du DPO externe et obtenir des dommages et intérêts. C'est pourquoi certaines assurances proposent une assurance responsabilité civile professionnelle pour les DPO.

Le DPO peut-il être licencié ou relevé de ses fonctions ?

Le délégué bénéficie d'un statut spécifique d'indépendance (voir fiche n° 6). Il ne peut pas être « relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions » (art. 38.3 du RGPD). Cette disposition signifie qu'un DPO ne peut être inquiété pour des analyses ou remarques fondées en matière de protection des données qu'il adresserait aux opérations de traitement de son employeur. Ainsi, au-delà du risque prud'homal, le licenciement abusif d'un DPO constituerait une infraction au RGPD.

Toutefois, le DPO n'est pas un salarié protégé au sens juridique, et ne dispose pas d'une procédure dédiée de licenciement prévue par le code du travail.

Il peut, comme tout autre salarié ou agent, être licencié pour des motifs autres que l'exercice de ses missions de délégué, par exemple en cas de vol, de harcèlement moral ou d'autres fautes graves similaires.

Enfin, l'organisme qui désigne un DPO doit s'assurer que ce dernier détient les qualifications et les capacités lui permettant d'accomplir ses missions. Il peut dès lors décider de retirer les missions de DPO à un salarié n'étant pas à même de remplir les missions qui lui sont attribuées par le RGPD.

Cette procédure n'est possible que si l'employeur s'est assuré que la difficulté du DPO à assurer ses missions ne vient pas d'une insuffisance des moyens – notamment temporels – qui lui sont accordés. Elle doit être documentée et réalisée selon les conditions fixées dans le contrat ou par son statut.

Quant au DPO externe, il peut également être mis fin à son contrat de prestataire conformément au droit des contrats ou de la commande publique et selon les conditions qui y sont fixées.

Le DPO doit-il être rattaché à une direction particulière ?

Le RGPD ne précise pas le niveau de « rattachement » du délégué qui peut donc dépendre de la direction des systèmes d'information (DSI), de la direction des risques, de la conformité, de la direction juridique ou encore du secrétariat général de l'organisme. Quelle que soit la direction à laquelle il est rattaché, il importe que le DPO soit en mesure de faire directement rapport au niveau le plus élevé de la direction de l'organisme afin que ses conseils soient connus et pris en compte.

Le DPO peut-il recevoir des consignes (telles que « réaliser un audit chaque année ») ou avoir des objectifs ?

Le DPO ne peut pas recevoir d'instructions sur la manière opérationnelle de décliner ses missions.

Ainsi, par exemple, un organisme ne peut interdire au DPO de contacter la CNIL pour avoir un conseil, l'obliger à approuver un document, ni dénaturer ou repousser sans cesse la communication qu'un DPO souhaiterait adresser aux employés ou agents de l'organisme. Sur ce sujet, la CNIL est déjà intervenue auprès d'organismes pour leur rappeler leurs obligations.

Il est possible de lui adresser des demandes (comme la production d'un rapport annuel, la rédaction d'un audit, etc.) dès lors que celles-ci ne l'empêchent pas d'avoir les ressources nécessaires, notamment en termes de disponibilité, pour mener à bien les autres missions que le DPO estimerait prioritaires. Ces missions pourraient alors être prévues dans la lettre de mission.

Il peut également avoir des objectifs évaluables, assortis de moyens suffisants pour les mener à bien, dès lors que ceux-ci sont établis en cohérence avec les actions qu'il a lui-même identifiées comme prioritaires, notamment dans le cadre de la sensibilisation des équipes internes.

L'indépendance du DPO ne doit pas, en effet, être comprise comme la possibilité pour le DPO de travailler de façon opaque, sans communication avec la direction ou les autres services sur les éléments qu'il a identifiés comme prioritaires ou sur les mesures qu'il compte mettre en place. C'est dans la liberté opérationnelle de définir ces priorités et ces mesures que l'indépendance se traduit : elle ne signifie pas l'absence de liens, mais l'absence de consignes qui auraient valeur d'ordre ou d'injonction dans la relation salariée ou hiérarchique.

Enfin, le DPO peut recevoir des consignes sur des éléments qui ne relèvent pas de l'exécution de ses missions, comme une obligation de faire valider ses congés dans un outil interne.

Des documents produits par le DPO peuvent-ils être « validés » ou modifiés ?

En indiquant que le DPO ne reçoit aucune instruction concernant l'exercice de ses missions et qu'il doit être capable de faire directement rapport au niveau le plus élevé de la direction, le RGPD met le DPO en capacité de produire tout document (élément de formation, rapport, expertise, etc.) sans interférence, en particulier sur le fond.

Il peut cependant décider de lui-même de soumettre un travail préparatoire à sa hiérarchie ou d'autres services pour recevoir des commentaires ou des remarques qu'il peut choisir de prendre en compte ou non.

TEXTES OFFICIELS

Sur cnil.fr :
- Article 38.2 et 38.3 du RGPD sur la fonction de DPO.
- Articles 226-26 à 226-24 du code pénal.

Fiche 7 : Que faire en cas de départ, de congés ou de remplacement du DPO ?

Le délégué joue un rôle central dans la protection des données de l'organisme, et fait office de point de contact pour les personnes ainsi que pour l'autorité de contrôle avec laquelle il doit coopérer. Par conséquent, le départ ou le remplacement d'un DPO, qu'il soit définitif ou temporaire, doit être anticipé et organisé par le responsable de traitement le plus en amont possible.

La transition en interne

Communiquer en interne : de la même manière que lors de sa désignation, le départ et le remplacement du DPO nécessitent d'être relayés en interne par tous moyens (exemple : note interne publiée sur l'intranet, information des instances représentatives du personnel, etc.).

En cas de remplacement, cette information permettra de communiquer le nom et les coordonnées du nouveau DPO.

Assurer le suivi des dossiers en cours : il est essentiel de mettre à jour les procédures permettant d'assurer le suivi et la reprise des dossiers en cours (exemple. : suivi d'une demande d'exercice de droit, réalisation d'une AIPD en cours, etc.).

La transparence vis-à-vis des personnes concernées

En cas de départ ou de remplacement, l'organisme doit s'assurer que les mentions d'information, qui doivent comporter les coordonnées du DPO, sont à jour.

À noter : pour éviter cette mise à jour systématique des mentions d'information, privilégiez des coordonnées « neutres » (exemple : adresse email générique, numéro de téléphone, adresse postale, etc.).

Les démarches auprès de l'autorité de contrôle

En cas de changement définitif

Le responsable de traitement ou le sous-traitant doit, dans les meilleurs délais, informer la CNIL de la fin de mission de son DPO. De façon opérationnelle, pour traiter une fin de mission, il est demandé de mettre le représentant légal en copie du courriel informant la CNIL de la fin de mission (voir adresse dans le courriel de confirmation de la désignation).

Si le DPO est remplacé, l'organisme doit, dans les mêmes délais, procéder à la désignation du nouveau DPO (voir fiche n° 4).

En cas d'absence temporaire

- **Si le DPO absent est officiellement remplacé par un autre DPO le temps de son absence**, une nouvelle désignation est alors requise auprès de la CNIL (en informant dans le même temps de la fin de mission du DPO absent) ;
- **si le DPO n'est pas remplacé**, il est nécessaire de prévoir une mise à jour des procédures internes (exemple : routage du courrier et des appels) garantissant que les demandes des personnes concernées ou de l'autorité de contrôle soient traitées. Dans les cas où la nomination du délégué est obligatoire pour l'organisme, cette vacance ne peut être qu'exceptionnelle et très limitée dans le temps.

À noter : lorsque la CNIL prend contact avec un organisme, elle s'adresse au DPO officiellement désigné auprès de ses services indépendamment des réorganisations internes mises en place. Il est donc important de gérer l'orientation des appels et courriers vers les personnes compétentes le temps d'une désignation pérenne.

Questions fréquentes

Un DPO peut-il demander la fin de sa mission tout en restant dans l'organisme ?

La CNIL recommande de prévoir lors de la prise de fonction, dans la lettre de mission ou dans le contrat, les conditions et modalités de la fin de mission demandée par le salarié DPO. Cela permet aux deux parties de confirmer que le DPO ne sera pas pénalisé ou freiné par sa mission dans le déroulement de sa carrière, et qu'il peut bénéficier des mêmes opportunités de promotions ou de mobilité interne que ses collègues.

TEXTES OFFICIELS

Sur cnil.fr :
- Article 39.1 du RGPD (missions du DPO).
- Article 38.3 du RGPD (indépendance du DPO).
- Articles 83 du décret d'application de la loi Informatique et Libertés (modalités de désignation du DPO auprès de la CNIL).

COMMENT LA CNIL ACCOMPAGNE-T-ELLE LES DPO ?

La CNIL accompagne les DPO en mettant à leur disposition différents outils, que l'on peut classer dans les deux catégories suivantes :

Les outils pour se former

- **Le site** www.cnil.fr **:** constamment alimenté, il contient de nombreuses informations, classées notamment par démarches, thématiques, technologies ou textes officiels. Les publications régulières de communiqués et d'actualités assurent une actualisation des connaissances. Un moteur de recherche ainsi qu'un outil « besoin d'aide » permettent également de répondre aux demandes ciblées.
- **Les ateliers ou webinaires :** ils sont accessibles à tous les professionnels de la protection des données sous réserve d'inscription préalable via le site web de la CNIL. Ils se concentrent sur une thématique (marketing, ressources humaines, recherche dans le domaine de la santé, etc.) qu'ils examinent en profondeur, ménageant également un temps pour les questions.
- **Une formation en ligne (MOOC)**, portant sur les fondamentaux de la protection des données, « L'Atelier RGPD », ouvert à tous et gratuit, a été publié en mars 2019. Face au succès rencontré (plus de 100 000 comptes créés à fin 2020), cet outil sera prochainement traduit en anglais et enrichi de modules thématiques spécifiques, à commencer par un module à destination des collectivités territoriales.

Les outils pour trouver une réponse

- **Une permanence téléphonique :** les agents du service des DPO assurent une permanence les lundis, mardis, jeudis et vendredis de 10h à 12h au 01 53 73 22 22 (touche 3), réservée aux délégués désignés.
- **Une adresse électronique dédiée :** l'adresse du service des DPO (figurant dans le message électronique confirmant la désignation) permet d'obtenir une réponse écrite aux demandes de conseil pour lesquelles le délégué n'a pas trouvé les éléments souhaités sur le site de la CNIL, ou qui n'auraient pas déjà été traitées par un réseau de professionnels de son secteur.

> Vous êtes particulièrement nombreux à nous solliciter par email ou par téléphone : il est donc indispensable de consulter notre site web et de mener votre propre analyse avant de nous contacter.
> En accord avec la charte d'accompagnement de la CNIL, le service DPO répondra en priorité aux questions dont la réponse ne se trouve pas sur cnil.fr.

- **Les réseaux professionnels de DPO :** ce sont de bonnes sources de réponse aux questions « terrain ». Organisés par secteurs et par régions, ils peuvent apporter un retour d'expérience ou de précieux conseils. Dans le cadre de sa stratégie de dialogue prioritaire avec les « têtes de réseau », ces réseaux professionnels sont des interlocuteurs privilégiés de la CNIL.

Les outils d'aide à la mise en conformité

- **Un modèle de registre simplifié :** les DPO sont le plus souvent au cœur de la réalisation de cet outil à la fois obligatoire et essentiel pour le pilotage de la conformité (voir « Le DPO et la documentation »). La CNIL propose un modèle de registre réutilisable, en format ouvert, comprenant une fiche tutorielle, une fiche de liste de traitements, un modèle de fiche à remplir et une fiche d'exemple. Elle a également **publié** son propre registre, utilisable comme exemple concret pour comprendre les enjeux et une manière possible d'utiliser cet outil.
- Pour la réalisation d'analyse d'impact relative à la protection des données, la CNIL propose un outil PIA prêt à l'emploi permettant de piloter une AIPD de A à Z. Elle a également publié des guides pour accompagner les responsables de traitements et les DPO dans cette obligation, ainsi que des listes de traitements pour lesquels les AIPD sont obligatoires ou, au contraire, non requises.
- La CNIL publie de nombreux documents, rappelant le droit en vigueur, synthétisant sa doctrine ou apportant de bonnes pratiques. En se rendant régulièrement sur son site, le DPO peut prendre connaissance des packs de conformités, des référentiels, des lignes directrices, etc.
- Enfin, étant au centre de la mise en conformité avec le RGPD, le DPO peut trouver un intérêt dans tous les outils publiés par la CNIL, pour dialoguer efficacement avec ses collègues (par exemple avec le « Guide RGPD du développeur ») ou pour mieux comprendre les obligations incombant à son organisme (comme le « Guide pratique sur les durées de conservation » peut le permettre).

FOCUS : « DPO : PAR OÙ COMMENCER ? »

Vous venez d'être désigné délégué à la protection des données : quelles devront être vos premières actions ? Comment prioriser les différents projets ?

La page « DPO : par où commencer ? » du site web de la CNIL vous propose un plan de travail permettant de procéder avec méthode pour aider les organismes à remplir leurs obligations, en proposant notamment un plan d'accompagnement qui permet de cartographier les traitements et prioriser les actions les plus urgentes.

Je recherche un DPO pour mon organisme, comment faire ?

Le choix d'un DPO peut être réalisé au sein des effectifs de votre organisme ou en faisant appel à un prestataire proposant ses services de DPO (le cas échéant, cette personne est également DPO d'autres organismes, on parle alors de DPO mutualisé).

L'organisme recrutant la personne doit s'assurer que celle-ci dispose de connaissances spécialisées du droit et des pratiques en matière de protection des données. Il doit ainsi prendre en compte les formations, longues ou courtes, suivies par la personne pressentie, mais également son expérience et sa connaissance du secteur. Des formations diplômantes en protection des données existent, mais elles ne sont ni obligatoires ni le seul moyen de devenir DPO ou d'être formé sur ces sujets.

Par ailleurs, afin d'accompagner les organismes dans l'identification du profil adapté, la CNIL a mis en place une procédure de certification des compétences du DPO sur la base d'un référentiel élaboré par la CNIL. Les certifications sont délivrées par des organismes certificateurs agréés par la CNIL. La liste de ces organismes est disponible sur notre site web.

Pour vérifier qu'un DPO est véritablement certifié, un recruteur peut contacter l'organisme de certification ayant attribué la certification. La CNIL ne détient pas de liste des DPO certifiés mais publie une liste des organismes de certification agréé.

Qu'apporte la désignation d'un DPO si mon organisme a déjà un service juridique compétent en matière de protection des données ?

Si un organisme rencontre des problématiques relatives à la protection des données personnelles, la CNIL recommande la désignation d'un DPO même lorsque celle-ci n'est pas obligatoire.

En effet, une équipe juridique, même compétente, ne peut se substituer aux avantages qu'apportent la désignation d'un DPO :

- il s'agit d'un point de contact facilement trouvable et joignable, en interne comme en externe ;
- il allie des connaissances juridiques et de sécurité informatique ;
- son indépendance, définie par un texte légal, assure son impartialité et la liberté de ses recommandations ;
- il peut bénéficier de soutien et d'une assistance de la CNIL.

Où le DPO doit-il être localisé ?

Le RGPD ne fixe pas d'exigence relative à la localisation du DPO. Cependant, le délégué doit être **facilement joignable** par les personnes concernées et les autorités de contrôle compétentes. Il est ainsi recommandé que le DPO se trouve dans l'Union européenne, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union européenne.

Si l'organisme ne possède pas d'établissement dans l'Union européenne, le délégué peut être établi hors Union européenne sous réserve qu'il puisse efficacement mener ses activités.

Quelle langue doit parler le DPO ?

Le délégué doit être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec les autorités de contrôle compétentes. Cela signifie que ces échanges devront se faire dans la ou les langues utilisées par les personnes concernées et les autorités de contrôle.

Pour répondre à cette exigence, le délégué peut, par exemple, se faire aider d'une équipe de relais locaux qui seront en capacité de répondre dans la langue des personnes concernées.

Des sociétés opèrent du démarchage auprès des professionnels (entreprises, administrations, associations), parfois de manière agressive, afin de vendre un service d'assistance à la mise en conformité au RGPD.

Pour rappel, la CNIL ne fait jamais payer de service de mise en conformité au RGPD. Elle ne demande jamais le règlement immédiat d'une somme d'argent dans le cadre d'un contrôle.

La CNIL et la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ont publié un communiqué pour aider les professionnels à se prémunir contre ces pratiques abusives.

Le titre de « délégué à la protection des données – DPO – DPD » est-il réservé aux personnes désignées auprès de la CNIL ?

Oui, ce titre ne peut être utilisé que par les personnes qui sont DPO au sens du RGPD, et, en particulier, désignées auprès de la CNIL. La personne désignée a le droit d'utiliser le logo « DPO » (marque protégée par la CNIL) dans l'exercice de ses fonctions.

Les responsables de traitement, en dehors des cas de désignation obligatoire, qui ne souhaitent pas désigner un délégué à la protection des données (DPO) sur la base du volontariat, peuvent employer une personne ou des consultants extérieurs, chargés des missions liées à la protection des données personnelles.

Dans ce cas, il importe de veiller à ce qu'il n'y ait pas de confusion quant à son titre, son statut, ses fonctions et ses missions. Aussi, il convient d'indiquer clairement, dans toute communication au sein de l'entreprise ainsi qu'avec les autorités chargées de la protection des données, les personnes concernées et le public (au sens large), que cette personne ou ce consultant ne porte pas le titre de délégué à la protection des données.

Pourquoi la CNIL utilise-t-elle l'abréviation « DPO » plutôt que « DPD » ?

La CNIL utilise toujours le nom de « délégué à la protection des données », la mention « DPO » n'intervenant qu'à titre accessoire pour abréviation.

L'abréviation des mots « *data protection officer* » désignant la fonction de délégué dans la version en anglais du RGPD apparait toutefois nécessaire à l'accessibilité de ses productions, afin de tenir compte de l'usage très répandu de cette abréviation dans les métiers du numérique et au sein du grand public.

L'emploi de l'abréviation « DPO » permet ainsi à la CNIL – conformément à l'une de ses missions – de toucher une large audience utilisant cette abréviation pour rechercher en ligne des publications relatives à la fonction de délégué à la protection des données.

Toutefois, il n'existe aucune restriction à utiliser l'abréviation DPD.

Comment un DPO peut-il se former ?

Pour acquérir les compétences et connaissances nécessaires à l'exercice du métier de DPO, le délégué peut notamment s'appuyer sur l'ensemble des ressources disponibles sur le site web de la CNIL.

La CNIL propose également des journées de présentation du RGPD et des ateliers d'information thématiques (sécurité, santé, AIPD, etc.), parfois délivrés sous forme de webinaires. Pour consulter les dates de ces événements et s'y inscrire, un agenda est mis à disposition sur le site web de la CNIL.

En mars 2019, la CNIL a lancé son MOOC, « L'Atelier RGPD », gratuit et à destination de tous les publics, mais suffisamment riche pour intéresser les DPO en formation. Celui-ci sera bientôt traduit en anglais et enrichi de nouveaux modules thématiques.

Le DPO peut également s'orienter vers des formations longues proposées par des universités ou des écoles (voir, entre autres, la liste des formations DPO réalisée par l'AFCDP[6] et la page dédiée sur le site de SupDPO[7]).

Selon l'étude sur les DPO réalisée par l'AFPA[8], les principaux contenus thématiques sur lesquels les DPO souhaitent pouvoir être formés sont des éléments de sécurité informatique (chiffrement, authentification forte, traçabilité, etc.), la réalisation des premières analyses d'impact et la connaissance des systèmes d'information (base de données, cloud, cookies, API, etc.).

6 Association française des correspondants à la protection des données à caractère personnel.
7 Association des DPO de l'Enseignement supérieur, de la recherche et de l'innovation.
8 « Délégué à la protection des données (DPO) : un métier qui se développe, une fonction qui se structure », étude réalisée par la direction prospective métier de l'AFPA, à la demande du ministère du Travail, de l'Emploi et de l'Inclusion (DGEFP), en partenariat avec la CNIL et l'AFCDP (2020).

Annexe n° 1 : Les questions clés à se poser lors de la désignation d'un DPO

- ☐ La personne pressentie connaît-elle les enjeux et a-t-elle un intérêt pour la protection des données et les missions d'un DPO ?
- ☐ Avez-vous vérifié que la qualité ou les missions préexistantes de la personne pressentie n'engendre pas un conflit d'intérêts ?
- ☐ La personne dispose-t-elle du niveau de connaissances (expertise juridique et technique en matière de protection des données, connaissances des pratiques de l'organisme et du secteur d'activité, etc.) et des compétences nécessaires (aptitude à savoir communiquer, etc.) ?
- ☐ Si cela est nécessaire, un plan de formation est-il programmé à cet effet ?
- ☐ Avez-vous établi une documentation permettant de justifier le choix de votre DPO (exemple : CV, éventuelle certification, etc.) ?
- ☐ Est-il prévu de communiquer en interne (salariés, IRP, etc.) sur la désignation du DPO ?
- ☐ Les missions et conditions d'exercice des missions du délégué sont-elles formalisées dans une lettre de mission ou un contrat de prestation de service ?
- ☐ Des garanties sont-elles prévues pour assurer l'indépendance du DPO (ne pas être sanctionné pour l'exercice de ses missions de DPO, ne pas recevoir d'instruction dans le cadre de l'exercice de ses missions de DPO) ?
- ☐ Une organisation est-elle mise en place pour permettre au DPO de faire directement rapport au niveau le plus élevé de l'organisme ?
- ☐ Une évaluation de la charge de travail du DPO et de ses besoins matériels (infrastructure, personnel supplémentaire, etc.) a-t-elle été menée ?
- ☐ L'accès aux données et aux opérations de traitement sera-t-il facilité ? Le DPO pourra-t-il accéder aux informations utiles ?
- ☐ Des moyens de contact permettant aux personnes concernées de joindre facilement le DPO ont-ils été mis en place (adresse email dédiée, ligne téléphonique, etc.) ?
- ☐ Le périmètre des missions du DPO est-il défini ? (exemple : tenue du registre, rédaction des clauses de sous-traitance, etc.) ?
- ☐ Avez-vous défini une gouvernance (niveau de mutualisation adéquat, mise en place de relais ou référents, formalisation des missions de ces relais, etc.) ?

Annexe n° 2 : Modèle de lettre de mission remise par l'organisme au DPO lors de sa prise de fonction

ATTENTION

Ce document est un modèle générique de lettre de mission qu'un organisme est susceptible de remettre à son DPO. Il doit être adapté aux spécificités du contexte (nature juridique de l'organisme, type d'activité, profil et positionnement du DPO) dans les limites du rôle et des missions du DPO définis par le RGPD.

[Nom de l'organisme] a désigné auprès de la CNIL, le [date], Mme / M. [Prénom, Nom, fonction le cas échéant], en tant que Délégué à la protection des données (DPO) tel que définit aux articles 37 et suivants du règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données (RGPD). Un récepissé de cette désignation a été transmis par la CNIL le [date].

À ce titre, Mme/M. [Prénom, nom du DPO] est en charge de veiller au respect des principes et des obligations en vigueur pour tous les traitements de données personnelles mis en œuvre par [Nom de l'organisme] ou pour son compte. Il tient compte dans l'exercice de sa mission du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités des traitements.

Dans le cadre de ses fonctions de DPO, Mme/M. [prénom, nom du DPO] fait directement rapport à [instance de direction de l'organisme/autorité]. Il a accès aux données personnelles et aux traitements mis en œuvre par [Nom de l'organisme] ou pour son compte. Il ne reçoit aucune instruction en ce qui concerne l'exercice de ses missions ni ne peut être pénalisé dans sa carrière en raison de celles-ci.

D'autres missions et tâches ne peuvent être attribuées à Mme/M. [Prénom, nom du DPO] que dans la mesure où elles ne sont pas susceptibles de créer des situations de conflit d'intérêts ou le prive des ressources nécessaires pour exercer sa mission de DPO.

Mme/M. [Prénom, nom du DPO] est soumis à une obligation de [secret professionnel / confidentialité]. Cette obligation ne doit cependant pas l'empêcher de demander conseil, dans l'exercice de ses missions, auprès de toute autorité ou personne compétente.

Chargé de veiller à la conformité des opérations de traitements de données personnelles, aux dispositions relatives à la protection des données personnelles, le DPO a notamment pour mission :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que les employés,
- de contrôler le respect du présent règlement et des dispositions en matière de protection des données,
- de 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,

- de coopérer avec l'autorité de contrôle,
- de faire office de point de contact sur les questions relatives au traitement des données personnelles.

[Dans la mesure où cela ne fait pas obstacle à la réalisation des missions précitées, le DPO est chargé des missions supplémentaires suivantes, avec l'aide des services concernés :

- tenir à jour le registre des activités de traitement effectuées par [Nom de l'organisme] ou pour son compte par un sous-traitant ;
- participer à la réalisation des analyses d'impact ;
- participer à la réalisation des notifications de violation de données personnelles ;
- remettre chaque année au responsable de traitement un rapport mensuel/biannuel/annuel des activités réalisées].

Afin de permettre l'accomplissement de ces missions, [nom de l'organisme] s'engage à ce que le DPO dispose des moyens adéquats et suffisants. Dans le cadre de l'exercice de ses fonctions de DPO, Mme/M. [prénom, nom du DPO] doit :

- accéder à l'ensemble des informations sur les projets ayant un impact sur les modalités de traitement des données personnelles dès leur origine (présence aux réunions transversales et métiers, etc.) ;
- accéder au niveau le plus élevé de la direction du responsable du traitement ;
- accéder à l'intégralité des systèmes d'information donnant lieu aux traitements de données personnelles par l'organisme ;
- bénéficier de formations régulières lui permettant d'entretenir ses connaissances spécialisées dans le domaine de la protection des données ;
- [disposer de moyens permettant de couvrir les besoins matériels et humains nécessaires à l'accomplissement de ses missions].

Une copie de cette lettre de mission sera diffusée à [l'ensemble du personnel et/ou des instances représentatives du personnel et/ou des organes décisionnaires de la structure].

[La confirmation de l'acceptation de cette lettre de mission devra être effectuée par courrier accompagné d'un exemplaire signé de la présente lettre.]

Signature du représentant légal de l'organisme **Signature du DPO**

Annexe n° 3 : Le formulaire de désignation du DPO

Le formulaire de désignation comprend 4 étapes :

- Étape 1 : informations sur l'organisme qui désigne un DPO ;
- Étape 2 : informations sur le délégué désigné ;
- Étape 3 : les informations publiques du délégué ;
- Étape 4 : récapitulatif et envoi à la CNIL

Le formulaire de désignation peut être complété par le représentant légal de l'organisme qui désigne le DPO, ou par toute autre personne spécifiquement mandatée par le représentant légal.

ATTENTION

La désignation d'un DPO emporte des conséquences juridiques. Le non-respect de l'une des dispositions relatives au DPO est susceptible d'être sanctionné. Il est donc impératif que le représentant légal du responsable de traitement ou du sous-traitant qui désigne le DPO soit informé de la démarche de désignation d'un DPO pour son organisme.

Étape n°1 : informations sur l'organisme qui désigne le DPO

OPTION 1 : L'ORGANISME DISPOSE D'UN NUMÉRO SIREN

Les informations concernant votre structure sont générées automatiquement depuis le répertoire SIRENE de l'Institut national de la statistique et des études économiques (INSEE).

Ces informations ne sont pas modifiables dans le formulaire. Il peut exister des variations sur l'effectif et le secteur d'activité, sans que cela n'ait d'impact sur la désignation du délégué.

En cas d'information erronée (exemple : adresse), rapprochez-vous des services de l'INSEE ou consultez leur site internet www.insee.fr (rubrique « immatriculer une entreprise, modifier sa situation ou déclarer sa cessation »).

OPTION 2 : L'ORGANISME NE DISPOSE PAS D'UN NUMÉRO SIREN

Cochez la case correspondante.

Vous devez renseigner manuellement les informations concernant la structure qui désigne le délégué.

À noter : le champ « Contact CNIL » : s'il ne s'agit pas du représentant légal lui-même, il doit s'agir d'une personne en contact avec ce dernier (exemple : assistant, directeur adjoint) que la CNIL peut contacter s'il est besoin de contacter le représentant légal.

Ce « contact CNIL » ne peut pas être le délégué.

Étape n°2 : informations sur le délégué désigné

OPTION N° 1 : LE DÉLÉGUÉ DÉSIGNÉ EST UNE PERSONNE PHYSIQUE.

OPTION N°2 : LE DÉLÉGUÉ DÉSIGNÉ EST UNE PERSONNE MORALE

- Soit l'organisme dispose d'un numéro SIREN : les informations de l'organisme sont générées automatiquement depuis la base SIRENE de l'INSEE (voir étape n°1).
- Soit l'organisme ne dispose pas d'un numéro SIREN : les informations devront être renseignées manuellement.

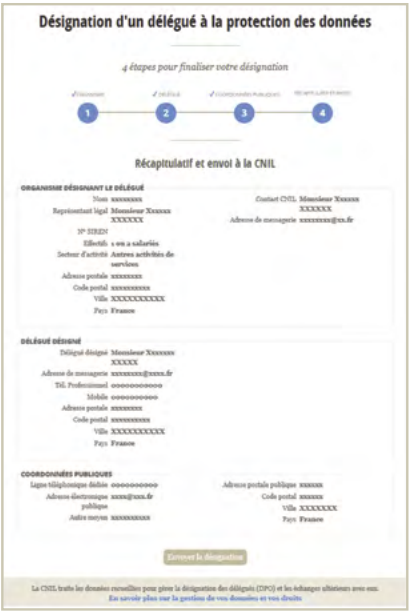
À noter : « *Coordonnées de la personne chargée de la désignation* » : il s'agit de la personne physique en interne qui exerce les missions du délégué.

Étape n°3 : les informations publiques du délégué

À cette étape du formulaire, il est demandé de renseigner deux moyens pour contacter le DPO. L'un d'eux doit être une adresse électronique ou un formulaire en ligne.

Ces informations sont mises à la disposition du public (open data) depuis le site de la CNIL. Ainsi, afin d'éviter de recevoir de trop nombreuses sollicitations, il peut être préférable d'inclure comme point de contact électronique l'adresse URL d'un formulaire en ligne.

En tout état de cause, ces coordonnées publiques n'ont pas à être identiques aux coordonnées uniquement accessibles aux services de la CNIL.



Étape n°4 : récapitulatif et envoi à la CNIL

Avant de valider la désignation, pensez à vérifier les informations renseignées dans le formulaire.

Après validation, vous pourrez télécharger un récapitulatif de la désignation au format PDF.

À noter : le responsable légal de l'organisme désignant le délégué, le contact de l'organisme pour la CNIL et le délégué désigné recevront un courrier électronique de confirmation.

ATTENTION

Il n'est pas nécessaire d'envoyer de document supplémentaire à la CNIL (exemple : lettre de mission, arrêté, délibération, etc.).

En cas d'erreur sur le formulaire, vous pouvez demander sa rectification en envoyant un courriel au service des DPO (dont l'adresse figure dans l'email confirmant la désignation du DPO).

ANNEXE N° 4 : Glossaire

AIPD : Analyse d'impact relative à la protection des données

API : *Application Programming Interface* (interface de programmation d'application)

CEPD : Comité européen de la protection des données

DPD / DPO : Délégué(e) à la protection des données / *Data protection officer*

RGPD : Règlement général sur la protection des données

RSSI : Responsable de la sécurité des systèmes d'information

Commission nationale
de l'informatique et des libertés
3, place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
Tél. : 01 53 73 22 22

www.cnil.fr
www.educnum.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS