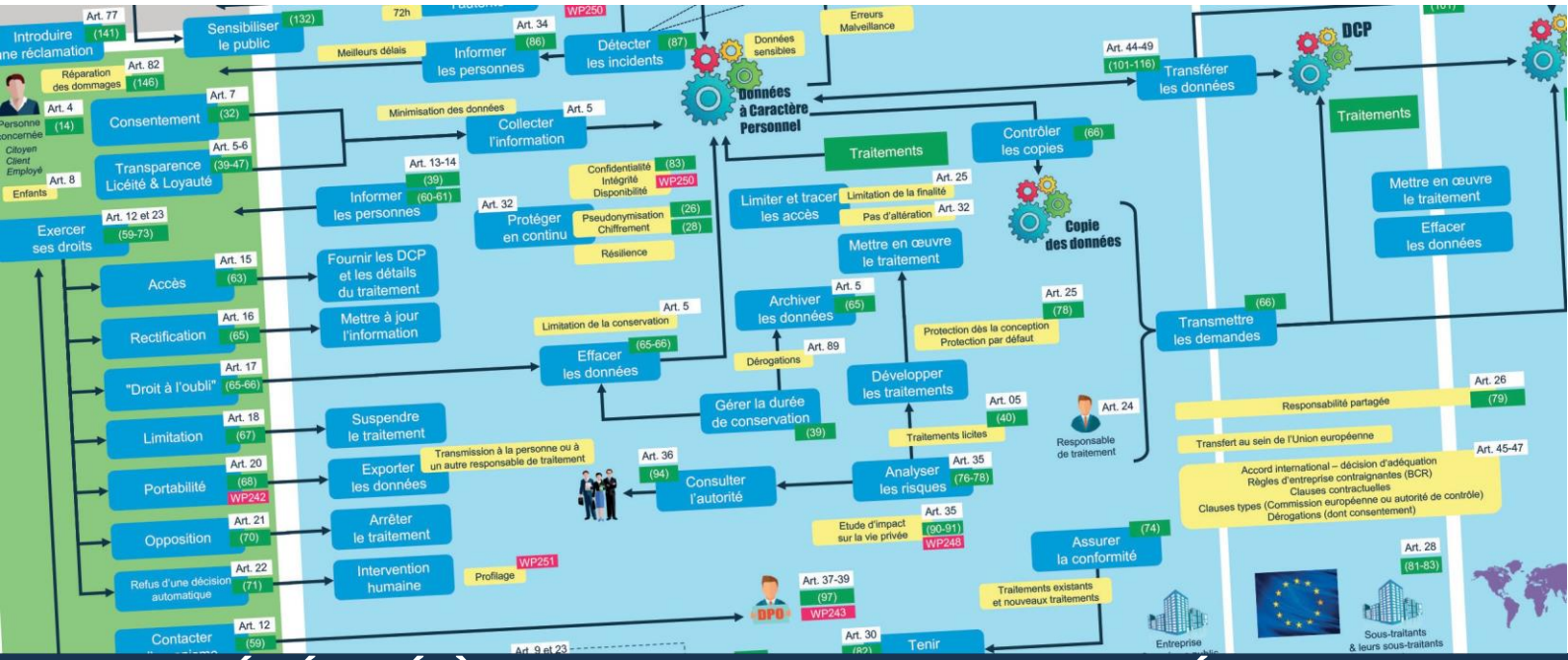
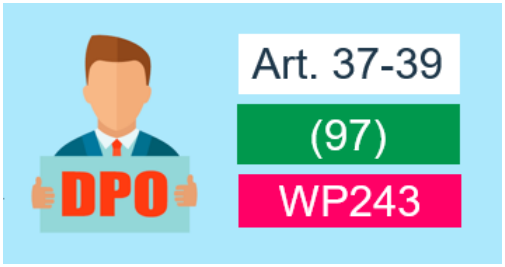
LES FICHES PRATIQUES du CLUSIF - RGPD



LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

QU'EST-CE QU'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES ?



Le règlement prévoit la nomination d'un Délégué à la Protection des Données. On utilise aussi souvent le terme anglais DPO (pour Data Protection Officer).
Trois articles du règlement lui sont consacrés :

- L'article 37 évoque sa désignation ;
- L'article 38 évoque sa fonction ;
- L'article 39 évoque ses missions.

Le DPO est chargé d'assister le responsable de traitement (RT) et les sous-traitants au respect du RGPD. Il est désigné sur la base de :

- Ses qualités professionnelles ;
- Ses connaissances spécialisées du droit ;
- Ses connaissances des pratiques en matière de protection des données ;
- Sa capacité à exercer ses missions.

Le RT veille à ce que le DPO soit associé à toutes les questions relatives à la protection des données à caractère personnel. Le RT fournit au DPO :

- Toute l'aide nécessaire ;
- Les ressources nécessaires ;
- L'accès aux données et aux opérations de traitement à caractère personnel ;
- Les moyens d'entretenir ses connaissances spécialisées.

Le DPO peut être externe à l'organisme sur la base d'un contrat de service.

1. QUEL EST LE RÔLE DU DPO ? QUELLES SONT SES MISSIONS ?

Le délégué à la protection des données reçoit plusieurs missions en application du règlement (*RGPD, Art. 39*) :

- Une mission d'avis et de conseil (a) ;
- Une mission de contrôle (b) ;
- Une mission de contact avec l'autorité de contrôle (c).

a. Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent en vertu du règlement et d'autres dispositions en matière de protection des données. Il doit aussi conseiller le responsable du traitement lorsque ce dernier est tenu d'effectuer une analyse d'impact relative à la protection des données conformément à l'article 35 ;

b. Contrôler la conformité des traitements au règlement, à d'autres dispositions de l'Union européenne ou de l'État membre concerné en matière de protection des données et aux règles internes du responsable du traitement ou du sous-traitant y compris la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux traitements, et les audits s'y rapportant ;

c. Être le point de contact de l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel, y compris concernant la consultation préalable visée à l'article 36, et consulter celle-ci, le cas échéant, sur tout autre sujet. Il doit bien entendu coopérer avec celle-ci.

Le règlement précise que le DPO tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement eu égard à la nature, à la portée, au contexte et aux finalités du traitement.

Les missions du DPO sont les suivantes :

- Informer et conseiller le responsable du traitement, le sous-traitant et les employés sur leurs obligations ;
- Contrôler le respect du règlement et des lois en vigueur (notamment la loi Informatique et Libertés), alerter si nécessaire et conseiller sur les mesures à prendre en cas de manquements ;
- Définir et contrôler les règles internes, préciser les responsabilités ;
- Tenir un inventaire des traitements de données à caractère personnel, en vérifier leur conformité au règlement, émettre des recommandations ;
- Sensibiliser et former le personnel participant aux opérations de traitement ;
- Veiller à la bonne réalisation des analyses d'impact relative à la protection des données ;
- Dispenser des conseils sur l'opportunité, la méthode, les modalités de réalisation, les mesures de sécurité techniques et organisationnelles ;
- Évaluer les opérations de traitement avec une approche par les risques ;
- Être le point de contact de l'autorité de contrôle (la CNIL en France) et coopérer avec elle ;
- S'assurer de la notification des éventuelles violations de données par le responsable de traitement ;
- Réaliser un bilan annuel des activités.

Le délégué à la protection des données peut également être amené à exécuter d'autres missions.

2. EXISTE-T-IL UNE FICHE DE POSTE TYPE POUR LE DPO ?

Le règlement est succinct sur la qualification attendue du délégué à la protection des données. Il indique (*RGPD, Art.37.5*) que celui-ci est *désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de ses capacités à accomplir les missions visées à l'article 39*.

Les lignes directrices du CEPD (anciennement G29, WP243) précisent les qualités attendues du délégué :

- Le délégué doit avoir une expertise et une compréhension approfondie du règlement et des lois et pratiques applicables en la matière ;
- Le niveau d'expertise attendu est fonction de la complexité des traitements, de leur ampleur et de leur sensibilité ;
- Au-delà de cette expertise technique (IT ou juridique), le DPO doit avoir une bonne connaissance de la structure dans laquelle il évolue et de son secteur d'activité ;

- Le DPO doit être un bon communicant afin de promouvoir une culture de la protection des données au sein de sa structure.

Selon le CLUSIF, ces qualités vont permettre au DPO de développer un réseau de relais et d'être mis dans la boucle dès le départ des projets. Il devra mettre en place une « culture d'entreprise ».
Il ne semble pas y avoir de profil type du DPO et il n'est pas forcément possible d'avoir toutes les compétences ou connaissances requises aussi il peut s'agir d'un travail d'équipe. Il sera alors amené à coordonner les acteurs de son entreprise et les actions des experts de son réseau, en veillant à la conformité.

La mission du DPO devrait en tout état de cause s'appuyer sur une lettre de mission qui légitime et encadre sa fonction. La fiche de poste devrait faire apparaître les missions liées à la fonction de DPO et ses activités devraient être mises en avant lors de l'évaluation annuelle. S'il s'agit d'une mission supplémentaire, comme dans le cas d'un RSSI qui cumulerait cette fonction avec celle de DPO, un avenant au contrat pourrait être envisagé mais il importe de distinguer le contrat de travail qui gère la relation avec l'entreprise, de la lettre de mission ou de la fiche de poste qui vont être déterminantes pour la relation en interne et les actions du DPO.

En complément : une fiche de poste DPO est proposée par l'AFCDP : https://www.afcdp.net/DPO-Fiche-de-poste-et-Lettre-de

> ⓘ ***Du point de vue du RSSI***
>
> Le RSSI traite de protection des données au sens large, et pas uniquement des données à caractère personnel. Au-delà du règlement, le RSSI doit ainsi intégrer de nombreuses réglementations, certaines globales, d'autres spécifiques au domaine d'activité ou à sa structure.
>
> En termes de profil : de la même façon qu'il n'y a pas un profil unique de DPO, le RSSI se révèle également un « mouton à cinq pattes », les profils de RSSI étant très nombreux. On trouve en revanche plus de propositions de fiches de poste type de RSSI, car la fonction est plus ancienne.
>
> On se reportera également à la section sur les synergies entre RSSI et DPO.

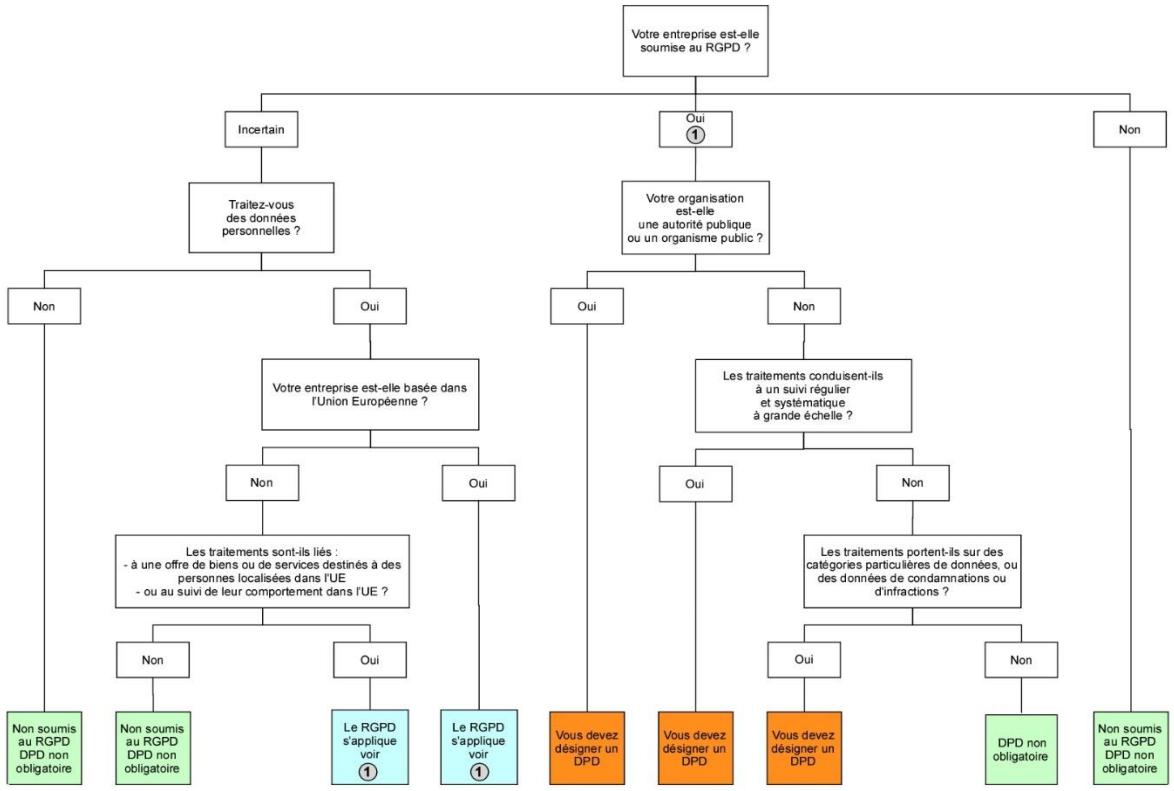
3. DOIT-ON NOMMER UN (OU PLUSIEURS) DPO ?

1. DANS QUEL CAS NOMMER UN DPO ?

Le règlement impose la désignation d'un délégué dans trois hypothèses (*RGPD, Art. 37*) :

- Lorsque le traitement est effectué par une autorité ou un organisme public, à l'exclusion des juridictions agissant dans le cadre de leur compétence judiciaire ;
- Lorsque les activités de base du responsable ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées ;
- Lorsque les activités de base du responsable ou du sous-traitant consistent en des traitements à grande échelle de données sensibles ou de données relatives à des condamnations et infractions pénales.

Dans les autres cas, il reste toutefois recommandé de désigner un DPO au sein de son organisme ou de sa structure.



2. QUE DEVIENT LE CIL ?

En France, la loi Informatique et Libertés avait créé le statut de correspondant Informatique et Libertés (CIL) chargé d'assurer, d'une manière indépendante, le respect des obligations prévues par la loi. Son statut et ses fonctions étaient fixés par la loi Informatique et Libertés, ainsi que par les articles 42 à 55 du décret n° 2005-1309 du 20 octobre 2005.

Le CIL disparaît et une nouvelle fonction est créée par le règlement, celle de délégué à la protection des données (DPO).

Une nouvelle désignation s'impose et le CIL ne devient pas automatiquement délégué à la protection des données. Le CIL a vocation à devenir DPO si ses compétences le permettent, si l'entreprise le souhaite, et s'il le souhaite lui-même.

3. LE DÉLÉGUÉ DOIT-IL ÊTRE DÉSIGNÉ EN INTERNE OU PEUT-IL ÊTRE EXTERNE À LA STRUCTURE ?

Le délégué à la protection des données peut être externe (*RGPD, Art. 37.6*) : « *le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service* ».

Les lignes directrices du CEPD (anciennement G29, *WP243*) précisent que si la fonction de DPO est assurée par un prestataire externe, les tâches peuvent être en pratique réalisées par une équipe (*WP 243 - Annexe, question 7*).

4. COMMENT NOMMER UN DPO ?

Le délégué à la protection des données doit être désigné auprès de l'autorité de contrôle. En France, la CNIL où la désignation peut être réalisée en ligne : https://designations.cnil.fr/dpo/

Le règlement oblige également le RT à publier les coordonnées relatives au délégué et à les communiquer à l'autorité de contrôle (*RGPD, Art. 37.7*).

Par ailleurs, le CEPD (anciennement G29) a pris le soin de préciser que la fonction de DPO ne pourra être revendiquée que par ceux qui auront fait l'objet d'une désignation à ce titre auprès de l'autorité compétente. Ainsi, par exemple, dans le cadre de communications externes, la référence à la fonction de DPO ne pourra être utilisée que s'il a été effectivement désigné. Cette même limite devra être prise en compte dans le cadre de la réalisation d'actions de communications ayant vocation à promouvoir la présence d'un DPO au sein d'une entité.

5. QUEL RATTACHMENT DU DPO ?

Le rattachement du délégué à la protection des données dépend du contexte de l'entité dans laquelle il exerce ses missions. Qu'il soit salarié de l'entité qui l'a désigné ou externe, l'essentiel est que le DPO puisse exercer ses missions et que son rattachement ne fasse pas obstacle notamment au principe d'indépendance ou encore que celui-ci ne soit pas placé dans une situation de conflit d'intérêts.

Le DPO doit en outre pouvoir bénéficier d'un degré d'autonomie dans l'exercice de ses missions (*RGPD, Art. 38.3, C97, WP243, chapitre 3.3*). En effet, compte tenu de ses obligations, il doit pouvoir exercer sa fonction en toute indépendance, sans recevoir d'instructions sur l'analyse à réaliser d'un traitement de données à caractère personnel ou sur le résultat souhaité à l'issue de celle-ci. De même, le DPO doit être en mesure de formuler ses recommandations et avis sur les traitements de données à caractère personnel que ceux-ci divergent ou non des avis d'autres parties prenantes dans le traitement.

Afin de définir le rattachement adéquat, il faut aussi tenir compte de ce que le délégué doit pouvoir procéder à des vérifications du respect du règlement par l'entité qui l'a désigné.
Autre signe d'indépendance, le DPO *fait directement rapport au niveau le plus élevé* de la direction de l'entité. L'objectif est que les organes de décision puissent être alertés des éventuels risques ou réserves que le DPO pourrait formuler. De cette manière, ces organes seront éclairés et en mesure de prendre les arbitrages nécessaires en matière de protection des données à caractère personnel.

Dans le cadre d'un DPO externe, son rattachement pourra être précisé dans le contrat de prestations de service qui le liera au RT ou au sous-traitant qui l'aura désigné.

6. QUELS SONT LES CAS DE CONFLITS D'INTÉRÊTS ?

Les missions du DPO comportent en particulier (*RGPD, Art. 39.1.b*) celle de *contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant.*

Selon le CLUSIF, il parait légitime que le DPO ne puisse se trouver en position de contrôler ses propres activités, ce qui le mettrait en situation de « conflit d'intérêts ». Le règlement prévoit d'ailleurs (*RGPD, Art. 38.6*) que si le délégué *peut exécuter d'autres missions et tâches*, il est toutefois nécessaire de veiller *à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts*.

Cette notion de conflit d'intérêts a été précisée par le CEPD (anciennement G29) dans ses lignes directrices concernant les délégués à la protection des données, adoptées dans leur version révisée le 5 avril 2017 (*Art. 3.5*). Le CEPD y rappelle que l'absence de conflit d'intérêts est indissociable de l'indépendance dont le DPO doit bénéficier dans l'exercice de ses missions.

Cela signifie en particulier que les autres missions du DPO ne doivent pas le conduire à *déterminer les finalités et les moyens [d'un] traitement de données à caractère personnel*. Loin d'être universel, cet aspect ne peut être étudié qu'au cas par cas, en fonction de l'organisation de chaque structure.

D'une manière générale, les fonctions exclues sont d'abord les fonctions d'encadrement supérieur (directeur général, directeur opérationnel, directeur financier, directeur marketing, directeur des ressources humaines ou DSI). Mais d'autres rôles de niveau inférieur dans la hiérarchie sont concernés, s'ils supposent la détermination de finalités et de moyens de traitements.

> ⓘ ***Du point de vue du RSSI***
>
> Dans le cas du RSSI, le conflit d'intérêts peut donc exister si ses missions comportent la définition et la mise en œuvre de certains outils de traitement. Il faut donc certainement faire la différence entre deux types de RSSI : ceux dont les missions sont très opérationnelles, et comportent par exemple le choix et la mise en œuvre de solutions de filtrage, de contrôle d'accès, de gestion de journaux, etc. Et ceux dont la mission est plutôt orientée vers le pilotage et la supervision, avec la définition de procédures et de politiques, et le contrôle de leur bonne mise en œuvre.
>
> Dans ce dernier cas, les missions de RSSI et celles de DPO telles que définies par le règlement (*RGPD, Art. 39.1*) sont d'ailleurs très similaires et complémentaires : informer et conseiller la gouvernance et les collaborateurs, contrôler le respect des textes officiels et des politiques internes, conseiller sur les analyses d'impact, coopérer avec les autorités…

7. QUELLE RESPONSABILITÉ JURIDIQUE POUR LE DPO ?

Il n'existe pas de responsabilité juridique spécifique du DPO : il convient de rappeler que seul le responsable du traitement ou le sous-traitant devra répondre des manquements relatifs à la protection des données constatés par l'autorité de contrôle. En effet, les obligations définies par le règlement sont uniquement et seulement mises à la charge des responsables du traitement et des sous-traitants.

À ce titre, il convient de souligner qu'une délégation de pouvoir qui transférerait au DPO, qu'il soit interne ou externe, la responsabilité incombant à ces derniers ne sera pas valable, le DPO étant de ce fait juge et partie. Partant, un conflit d'intérêt pourrait être constaté par l'autorité de contrôle.

En outre, les vérifications réalisées par le DPO dans le cadre de l'exercice de sa mission de contrôle du respect du règlement par l'entité qui l'a désigné et, plus généralement, de toute disposition relative à la protection des données – ce qui inclut les lignes directrices, guides, politiques et/ou procédures élaborés en interne – n'auront pas davantage pour effet de lui conférer la responsabilité des manquements qu'il pourrait constater.

8. Y A-T-IL UNE INFLUENCE DU DPO SUR LE MONTANT DE L'AMENDE EN CAS DE MANQUEMENT ?

Les lignes directrices du CEPD (anciennement G29, *WP253, Application et fixation des amendes*) précisent que si un traitement a été autorisé contre l'avis du DPO il peut être considéré comme une violation délibérée, et ouvrir à des sanctions plus importantes.

LES FICHES PRATIQUES

L'intégralité de la FAQ RGPD (version 2018) et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF