

PRINCIPES DE BASE DE LA PROTECTION DES DONNÉES

Les rôles en matière de Protection des données

Les acteurs du traitement de données

1 Personne concernée (ou individu ou « data subject »)

Terme technique désignant la personne sur laquelle portent des données personnelles particulières.

Une **personne physique** (c'est-à-dire un **individu**) dont **les données personnelles font l'objet d'un traitement**, qui peut être **identifiée, directement ou indirectement**, par référence à ces données.

Ex : traditionnellement les populations affectées et les employé·es.

2 Responsable de traitement (ou « data controller »)

Désigne la personne ou l'organisation qui, seule ou conjointement avec d'autres, détermine **les finalités et les moyens du traitement des données personnelles** (CICR).

Un responsable de traitement décide comment et pourquoi collecter et utiliser les données.



2 Responsable de traitement (ou « data controller »)

Voici 6 bonnes pratiques de la CNIL lorsqu'une organisation responsable de traitement travaille avec une organisation sous-traitante, par exemple un partenaire local :

- **Définir des rôles et responsabilités** précises dans le traitement des données
- Les formaliser dans un **contrat de sous-traitance clair**
- S'assurer que les **activités de traitements des données sont enregistrées et documentées (registre)** par l'organisation sous-traitante
- **Vérifier que l'organisation sous-traitante respecte la protection des données** (incluant la sécurité des données) ou l'accompagner dans ce sens
- **Veiller à ce que l'organisation sous-traitante permette l'exercice des droits des personnes concernées**

2 Responsable de traitement (ou « data controller »)

Voici les missions de responsable de traitement :

- décider de la **finalité de l'usage des données personnelles** et des moyens mis en place pour traiter la donnée
- si le traitement (en partie ou totalement) des données est « délégué » à un partenaire local, alors un contrat est nécessaire pour bien clarifier les responsabilités de chacun.e. Dans ce cas, votre organisation s'assure qu'il y ait des « garanties suffisantes » pour mettre en œuvre l'utilisation des données (par exemple, vérifier les compétences spécialisées sur la protection des données et la fiabilité de la personne/organisation)
- **suivre les activités de traitement des données** via l'outil du registre des traitements des données, qui permet de documenter et d'avoir une traçabilité des activités de traitements des données que vous réalisez au sein de l'organisation.

Les acteurs du traitement de données

2 Responsable de traitement (ou « data controller »)

- mettre en place des systèmes permettant aux personnes dont les données personnelles sont collectées, de pouvoir exercer leurs droits (par exemple, droit d'opposition ou de modification par exemple, via des mécanismes de feedbacks ou de réception de plaintes)
- informer l'autorité de contrôle (en France c'est la CNIL/ [lien pour trouver l'autorité de contrôle d'un autre pays de l'UE](#)/ au Royaume-Uni c'est le ICO) en cas de manquement à la protection des données personnelles (dans les 72 heures)
- fixer la durée de conservation des données personnelles, en fonction des utilisations nécessaires pour mener à bien le projet et des étapes (collecte, déploiement du projet, reporting, audit)

Les acteurs du traitement de données

3 Sous-traitant·e (ou « data processor »)

Désigne la personne ou l'organisation qui **traite les données personnelles pour le compte du ou de la responsable de traitement** (CICR).

Un **sous-traitant** est une personne ou une organisation distincte (pas un employé) qui **traite les données pour le compte du ou de la responsable de traitement et conformément à ses instructions**.

Une personne ou une organisation qui **traite et ajoute de la valeur** aux données brutes, par exemple en les nettoyant, en les chargeant dans une base de données consultable ou en les combinant avec des données provenant d'autres sources (OCHA).

Les acteurs du traitement de données

3 Sous-traitant·e (ou « data processor »)

Les sous-traitant·es ont certaines obligations légales directes, mais elles sont plus limitées que celles du responsable du traitement.

- Connaître les règles liées à la **protection des données** et avoir la **capacité de mettre en œuvre les traitements demandés** par le/la responsable de traitement
- **Alerter et informer le/la responsable de traitement si ses demandes sont illégales ou manquent de clarté** / si une personne souhaite exercer ses droits (par exemple de modification ou retrait)
- Tenir et suivre des **registres des activités de traitement des données personnelles** et de fuites de données
- Assurer la **sécurité des données**: avoir une méthode de travail basée sur la confidentialité, être transparent·e s'il y a une fuite/violation de données et renvoyer et détruire toutes les données au terme de sa mission
- **Désigner un·e DPO pour recevoir des conseils et de l'aide** pour respecter la protection des données

Les acteurs du traitement de données

4 Contrôleur·euse conjoint des données (ou « joint data controller »)

Si deux ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement des mêmes données personnelles, il·elle sont des contrôleur·euses conjoint·es.

Toutefois, ils ne sont pas des responsables de traitement conjoints s'ils traitent les mêmes données.

NB : cette situation peut exister dans les programmes en consortium. Ou plus simplement entre une ONG internationale et son partenaire local.



5 Sous-traitant·e tierce (ou « third-party data processor »)

Une personne ou une organisation engagée en son nom propre par un sous-traitant en charge du traitement des données pour un partenaire.

Ex : la contractualisation de consultants par CartONG pour travailler sur un projet.

Les acteurs du traitement de données

6 Délégué·e à la Protection des Données (« DPO »)

Elle·il a **un rôle de pilotage** de la mise en conformité des pratiques en respect avec la protection des données. Son poste peut-être en externe ou en interne à l'organisation.

Le·la **DPO doit rester indépendant·e**, être expert·e en matière de protection des données, disposer de ressources suffisantes et rendre compte au plus haut niveau de la direction.

Au-delà de son mandat à l'échelle du siège de son organisation, vis-à-vis des opérations terrains des ONG de solidarité internationale, on peut résumer ses missions à :

- Avoir un **rôle de conseil et d'information** en lien avec la protection des données au sein de l'organisation et avec les organisations liées
- De **contrôler l'application du RGPD et du droit national en matière de protection des données**

Pour remplir son rôle sur le terrain, le·la DPO a besoin de relais: il est recommandé d'avoir des points focaux



6 Délégué·e à la Protection des Données (« DPO »)

La désignation d'un·e DPO **étant obligatoire** pour les organisations dont les activités de base les amènent à **traiter à grande échelle des données dites « sensibles »** ou les organisations dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle.

Il est donc rare que des ONG de solidarité internationale d'une certaine taille ne soient pas concernées par l'obligation de désigner un·e DPO.

Remerciements

Cette présentation bénéficie du soutien de l'Agence Française de Développement (AFD) et du Centre de crise et de soutien du Ministère de l'Europe et des Affaires étrangères (CDCS). Néanmoins, les idées et les opinions présentées dans cette présentation ne représentent pas nécessairement celles de l'AFD ou du CDCS.

Cette présentation a été conçue en utilisant des ressources de [Flaticon](#), [Freepik](#) et de [The Noun Project](#).