

📖 le RGPD décodé

Règlement Général sur la Protection des Données

📄 **Texte de référence européen en matière de protection des données personnelles pour les résidents de l'Union Européenne, applicable depuis le 25 mai 2018.**

Sert à harmoniser la régulation des données personnelles dans l'ensemble des pays de l'U.E.

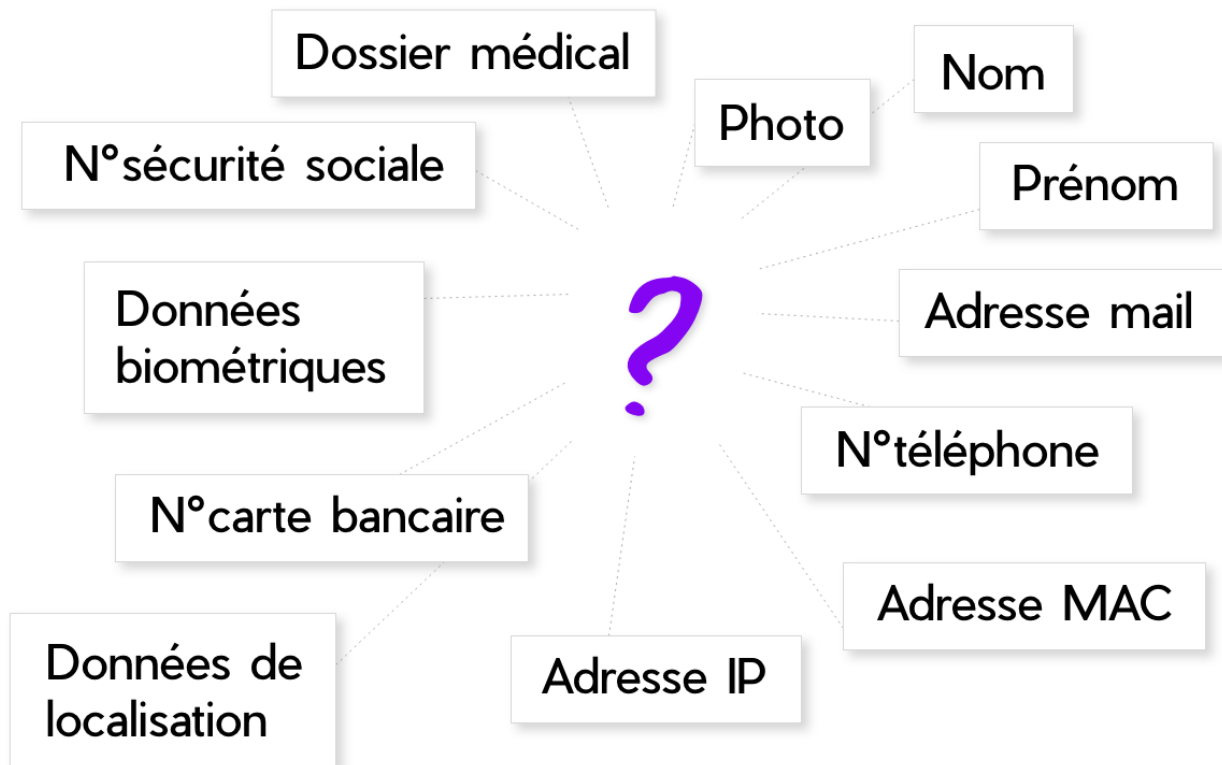
📄 **Ce règlement s'applique quand :**

- une organisation traite des données personnelles
- une organisation **hors U.E. traite des données personnelles de personnes résidentes de l'U.E.**

📄 **Le RGPD s'applique à tous les organismes, quelque soit leur taille, leur secteur ou leur caractère public ou privé.**

Données à caractère personnel

... Késako ☐ ? ? ?



☐ Tout ce qui permet de **deibler, suivre, surveiller, profiler** une personne est considéré comme **donnée personnelle**.

☐ Toutes données qui **parlent de notre activité**, qui sont **reliées à une personne**, directement ou indirectement sont des **données à caractère personnel**. Elles **permettent d'identifier une personne**.

☐ On associe souvent RGPD au web, et aux **cookies** ☐, mais le RGPD est aussi existant là où il n'y a pas de site internet, dès qu'une entreprise recueille des informations permettant d'identifier une personne même sur papier, elle se doit de respecter ce règlement.

Responsabilités partagées

Chez YWD, en tant qu'entreprise "sous-traitante", nous avons **une responsabilité propre** et **nous sommes tenus de respecter des obligations spécifiques de conseils et d'aide au respect du RGPD** à l'égard de nos clients.

L'entreprise qui fait appel à nos services pour un site internet n'est pas la seule responsable de ces données, **nous le sommes également**.

En cas de manquement au RGPD sur le site de notre client, nous pouvons être sanctionnés au même titre que notre client.

Donc, il est important de prendre le temps pour cette étape de mise en conformité d'un site ou d'une application.

Mais concrètement, on met quoi en place pour un site ?

1 Prévoir des mentions d'informations :

C'est à dire informer de façon transparente les personnes sur :

- **l'auteur de la collecte**
- **la durée de conservation** des données
- **la finalité** des données collectée
- **l'exercice de leurs droits** (modification, suppression de leurs données)

Le RGPD impose une **information complète, précise, transparente, compréhensible et aisément accessible** des personnes concernées.

Les modalités de fourniture et de présentation de cette information **doivent être adaptées au contexte**.

Pour les responsables de traitement, cette transparence contribue à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

Ces [mentions d'informations](#) peuvent **revêtir différents aspects**, on les rencontre souvent sous une des ces formes :

- ☐ **bandeau cookies**
- ☐ **texte accompagnant** une case à cocher pour consentement (formulaire de contact, newsletter, ...)
- ☐ **page de "politique de confidentialité" ou "données personnelles"**, qui se trouve souvent dans le footer (pied de page) du site et qui sert de base d'information aisément accessible une fois que le bandeau cookies a disparu par exemple.

2 ☐ Prévoir un registre de traitement des données

L'organisation dont le site internet traite des données personnelles, **doit tenir un registre de traitement des ces données, qui contient :**

- l'inventaire des traitements
- l'objectif des traitements
- la durée de conservation des données
- les obligations légales (durée de conservation particulière comme pour les fiches de paies)

☐ **Ce registre** est un service que l'outil [Azeptio](#) propose et gère pour l'organisation.

En cas de contrôle par la CNIL, l'entreprise est en règle et peut alors présenter le registre.

Il est à noter que s'il s'agissait d'une association, sans site internet mais gérant des cartes d'adhérents par exemple et donc des données personnelles, elle doit également tenir un registre du traitement de ces données.

L'organisation doit être en mesure de répondre à des sollicitations d'une personne (de qui elle a récupéré des données) à accéder à ces informations, les modifier voir les supprimer. Et c'est grâce

à ce registre qu'elle pourra le faire.

3 Prévoir des clauses de protection des données

le cas échéant, si elles sont gérées par un sous-traitant.

Qu'est-ce qu'un DPO et à quelle est sa mission ?




Data Protection Officer ou **Délégué** à la **Protection** des **Données**

Le DPO est le chef d'orchestre de la conformité en matière de protection des données au sein d'une organisation.

Toutes les organisations quelles que soient leurs tailles ou leurs secteurs d'activité peuvent désigner un délégué à la protection des données.

Il est aussi possible (pour les petites structures) de faire appel à un délégué externe partagé avec plusieurs organismes.

Ses missions :

-  Informer et conseiller l'organisation et ses employés
-  ➔ Contrôler le respect du RGPD au sein de l'organisation
-  Être le point de contact avec la CNIL
- Conseiller l'organisme sur la réalisation de l'**étude d'impact** relative à la protection des données et d'en vérifier l'exécution dans le cas où l'on traite des données sensibles ou à risques, ou si l'on fait du tracking à grande échelle par exemple.

Le DPO est obligatoire pour :

- les organismes publics : *mairies, ministères, ...*

- les organisations dont les activités de bases exigent un suivi régulier et systématique à grande échelle des personnes concernées : *compagnies d'assurance, établissements bancaires, entreprises de pub ciblées sur internet, ...*
- les organisation traitant des données sensible à grande échelle : *centres hospitaliers, compagnies d'assurance, sites de rencontre, ...*

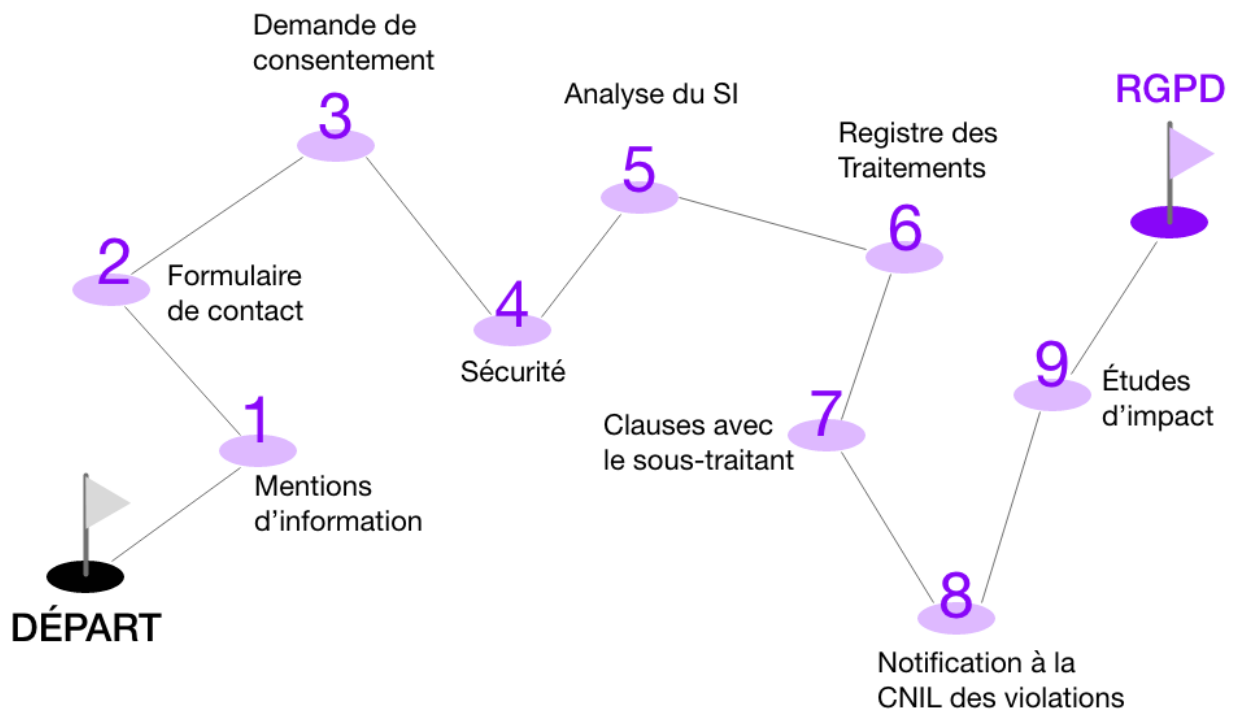
pour un savoir plus sur le DPO c'est [par ici](#) !

Comment prouver sa conformité au RGPD ?

Le plus important est de mettre en place les différentes actions et de prouver par une documentation écrite que l'on assure une protection des données en continue
= "accountability" ou "obligation de rendre compte".

En résumé : on doit montrer quelles actions on été mises en place et à les rendre vérifiables.

Exemple des différentes actions à mettre en place



Actions à mener dans un premier temps :

1. Informer les personnes sur la finalité de la collecte de leurs données.
2. Mettre en place un formulaire de contact pour que les personnes qui le souhaitent puissent accéder à l'ensemble des données qui les concernent.
3. Demander l'accord des personnes sur la collecte de leurs données et leur donner la possibilité de la refuser (demande de consentement cookies, newsletter, formulaire de contact du site, etc,...).
4. Mettre en place des mesures de sécurité adaptées à la sensibilité des données stockées dans le fichier. Pour en savoir plus [Guide de sécurité de la CNIL](#).

Actions à mener dans un second temps :

5. Analyser tous les documents et fichiers qui contiennent des données personnelles.
6. Créer un registre de traitement des données (service fourni par [Axeptio](#) | sinon la CNIL met à disposition une trame au format XLS [par là](#)).
7. Revoir les clauses passées avec un organisme, en cas de sous-traitance du traitement de données à caractère personnel. Des exemples de clauses ? c'est [juste ici](#) !
8. Si besoin, notifier à la CNIL, les violations de données dont l'entreprise est victime.
9. Dans certains cas spécifiques, comme le traitement de données sensibles ou à risque, ou encore en cas de tracking à grande échelle, l'organisme doit mener obligatoirement une [étude d'impact sur la protection des données](#) puisqu'il y a un risque élevé pour les personnes concernées. Cette étude va permettre d'anticiper et traiter les risques pour les droits et libertés de ces

personnes.

La CNIL a créée un [outil open source](#) pour aider les organismes dans la mise en place de cette analyse.

La CNIL a également édité [un guide](#) pour se préparer au RGPD.

Les sanctions pour manquement au RGPD

En cas de contrôle et de non conformité au RGPD, l'organisme encourt une amende allant jusqu'à **4% du chiffre d'affaires annuel mondial** ou **20 Millions d'euros**.

La sommes la plus importante entre les deux sera retenue.

Et si une personne me demande ses données ?...

Vous êtes dans l'obligation de transmettre les données concernant la personne.

Vous avez 1 mois maximum après réception de la demande, pour répondre à cette personne, et 2 mois si vous en informez la personne et que vous pouvez démontrer qu'il s'agit d'un processus complexe et nécessite un délais supplémentaire.

Sources : <https://www.cnil.fr/> | <https://www.youtube.com/watch?v=OUMGp3HHeI4>

Revision #3

Created 3 March 2023 17:09:55

Updated 20 November 2024 14:57:58 by Charline