# Règlement général sur la protection des données (RGPD)

## Table des matières

## Définition et cadre juridique

Le Règlement général sur la protection des données (RGPD) est, depuis le 25 mai 2018, le **nouveau cadre de référence européen** en matière de protection des données à caractère personnel. Il a pour objectif de mieux protéger les **données personnelles des citoyens européens** tout en imposant des **obligations supplémentaires** aux organisations publiques et privées qui **collectent**, **stockent**, **échangent** ou **transfèrent** ces données. Les organismes de recherche sont donc concernés par ce règlement.

### Qu'est-ce qu'une donnée personnelle ?

**Une donnée personnelle** est toute information se rapportant à une personne physique identifiée ou identifiable.

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image) ;
- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

**Les données sensibles** sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le Règlement européen interdit de recueillir ou d'utiliser ces données, **sauf**, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

### Qu'est-ce qu'un traitement de données personnelles ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

### Qu'est-ce qu'une analyse d'impact relative à la protection des données (AIPD) ?

Lorsqu'un traitement de données personnelles est susceptible d'engendrer **un risque élevé** pour les droits et libertés des personnes concernées, l'analyse d'impact relative à la protection des données est un outil obligatoire qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée.

L'AIPD doit être menée avant la mise en œuvre du traitement lorsque le traitement remplit **au moins deux** des neuf critères suivants :

- collecte de données sensibles ou données à caractère hautement personnel ;
- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.)
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

La CNIL a publié une liste de traitements (non exhaustive) pour lesquels l'AIPD est obligatoire.

## Si vous traitez des données à caractère personnel

**Ces données personnelles doivent être « traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) »** (article 5.1-a) du RGPD.

### Comment déclarer un traitement de données personnelles et se mettre en conformité ?

**Si dans le cadre de l'exercice d'un projet de recherche**, vous collectez ou utilisez des données à caractère personnel, ou si vous envisagez de le faire, vous devez solliciter le **délégué à la protection des données de votre organisme** (DPO) et **établir une fiche registre pour chaque activité de traitement qui lui sera transmise**.

> Dans ce cadre le document de référence est **le registre des activités de traitement** qui permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles. Il participe à la documentation de la conformité.

Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- les parties prenantes qui interviennent dans le traitement des données (représentant, sous-traitants, co-responsables, etc.);
- les catégories de données traitées ;
- à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées ;
- combien de temps vous les conservez ;
- comment elles sont sécurisées.

Ce document permet de vérifier que le traitement est licite et sécurisé.

### Que faire si vous collectez des données dans un territoire en dehors de l'Union européenne, si vos données sont transférées en dehors de l'Union Européenne ou si vous recevez des données d'une autre institution ?

Le règlement européen s'applique au traitement des données à caractère personnel effectué dans le cadre des **activités d'un établissement d'un responsable du traitement** ou d'un sous-traitant sur le territoire de l'Union, **que le traitement ait lieu ou non dans l'Union**.

Il s'applique également aux traitements effectués par un responsable de traitement ou un sous-traitant établis hors de l'Union européenne mais qui visent des personnes qui se trouvent sur le territoire de l'Union européenne.

*Par exemple, doivent respecter le RGPD :*

- ➔ *Un projet de recherche qui collecte des données de personnes sur le territoire européen pour ensuite les exporter*
- ➔ *Une projet de recherche qui collecte des données de personnes situées en dehors de l'U.E qui sont ensuite transférées sur le territoire U.E*
- ➔ *Un projet de recherche qui collecte des données personnelles hors de l'UE avec un responsable de traitement qui est situé sur le territoire de l'UE et qui réalise le traitement dans le cadre de ses activités.*

Dans tous ces cas, il est conseillé de contacter le DPO. Le transfert des données hors Union européenne est possible à condition d'assurer un niveau de protection suffisant et adapté et d'être encadré en utilisant différents outils juridiques.

## Régime juridique applicable aux projets de recherche

Le projet de recherche qui utilise des données personnelles doit respecter le RGPD et la loi Informatique et Libertés en plus des autres réglementations susceptibles de s'appliquer.

**La personne responsable du traitement détermine les finalités et les moyens d'un traitement**, c'est à dire l'objectif et la façon de le réaliser. En pratique, il s'agit de la personne morale incarnée par son représentant légal (le PDG). Cependant, celui qui est **responsable de la mise en œuvre du traitement (chercheur, agent etc.)** doit concilier les spécificités de son traitement avec l'impératif de protection des données à caractère personnel.

Avant d'engager son projet de recherche et lorsque celui-ci contient des données à caractère personnel, le responsable du projet scientifique engage l'analyse sur :

1. Les licéités et finalités du traitement ;
2. La pertinence et la proportionnalité des données ;
3. La sécurité, protection et confidentialité des données ;
4. La durée de conservation des données;
5. Transparence, consentement et information des personnes

**A ce titre, il doit remplir le registre de traitement avec les éléments justificatifs afin de vérifier sa conformité et le renvoyer au DPO.**

### *1. Licéités et finalités du traitement*

Le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime. Pour pouvoir être mis en œuvre, tout traitement de données doit se fonder sur l'une des « bases légales » prévues par le RGPD. C'est la licéité du traitement. **La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre**, ce qui donne le droit à un organisme de traiter des données à caractère personnel (par exemple pour un projet de recherche, le plus souvent la base légale sera soit le consentement, soit la mission d'intérêt public, soit l'intérêt légitime).

La finalité du traitement est l'objectif principal de l'utilisation de données personnelles. La finalité doit être en lien avec les missions de l'établissement ou de l'entité. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial. Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur.

### *2. Pertinence et Proportionnalité des données*

Les informations enregistrées doivent être pertinentes et **strictement nécessaires** au regard de la finalité du projet.

### *3. Sécurité, protection et confidentialité des données*

Le responsable de la mise en œuvre du traitement doit protéger les données et empêcher qu'elles soient volées, détournées ou réutilisées à des fins non prévues. Des mesures de sécurité sont mises en place quelle que soit la nature de la donnée, à toutes les étapes du projet.

Des mesures techniques et organisationnelles doivent être prises afin d'assurer la **sécurité et la confidentialité** des données :

- Le principe de pertinence et de minimisation des données traitées doit être respecté ;
- L'anonymisation des données (traitement permettant de rendre impossible, et cela de façon irréversible, l'identification des personnes) pourra être mise en œuvre (dans tous les cas, l'anonymisation est imposée lors de la diffusion des résultats) ;
- La pseudonymisation doit être mise en œuvre toutes les fois où cela s'avérerait pertinent ;
- Une logique d'accès sécurisé et contrôlé doit être développée (stockage, droit d'accès etc.).

- Seuls le responsable du projet et ses collaborateurs intervenant dans la recherche peuvent conserver **le lien entre l'identité codée** des personnes concernées par la recherche et leurs nom(s) et prénom(s) (table de correspondance conservée de façon sécurisée)[1].

### *4. Durée de conservation des données*

Les données à caractère personnel relatives aux personnes concernées par une recherche et traitées à cette fin ne peuvent être conservées dans les systèmes d'information du responsable de traitement, du centre participant ou du professionnel intervenant dans la recherche que **jusqu'à deux ans après la dernière publication des résultats de la recherche ou, en cas d'absence de publication, jusqu'à la signature du rapport final de la recherche.** Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une **durée de vingt ans maximum** ou pour une durée conforme à la réglementation en vigueur.

### *5. Transparence, consentement et information des personnes*

Les informations qui portent sur la finalité du traitement, le nom et les coordonnées du responsable du traitement, le nom et les coordonnées du délégué à la protection des données, les durées de conservation sont communiquées en toute **transparence** aux personnes concernées par le responsable du traitement des données. Elle doit être faite directement auprès des personnes concernées.

Le RGPD impose une information complète et précise. Les modalités de fourniture et de présentation de cette information doivent être adaptées au contexte. La transparence permet aux personnes concernées : de connaître la raison de la collecte des différentes données les concernant ; de comprendre le traitement qui sera fait de leurs données ; d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits (voir les exemples de mentions sur le site de la CNIL.)

→ droit d'accès à ses données ;
→ droit d'être informé d'une violation des données en cas de risque élevé pour les personnes concernées ;
→ droit d'opposition ;
→ droit de rectification ;
→ droit à l'effacement ;
→ droit à la portabilité ;
→ droit à une utilisation restreinte de ses données.

Toute personne peut exercer ces droits dès lors qu'elle connaît les noms et coordonnées du responsable de traitement et du Délégué à la protection des données, éléments qui sont obligatoires dans l'information faite aux personnes.
Des délais de réponse sont prévus par la règlementation : à compter de la réception de la demande d'accès aux données, la transmission de celles-ci doit se faire dans un délai d'un mois.

[1] *L'identification des personnes concernées au moyen d'un numéro d'ordre ou d'un code alphanumérique est nécessaire pour certifier que, pour chaque personne concernée, les informations recueillies successivement au cours de la recherche la concernent et vérifier, par la réalisation de contrôles de validité et de cohérence, la concordance des données recueillies au cours de la recherche avec celles des documents sources.*

## Régime juridique applicable aux projets de recherche : cas particulier des projets « santé »

La notion de **données de santé** est désormais définie par le RGPD, de manière large. En plus du RGPD (et donc les dispositions présentées dans le titre précédent), ces données de santé sont également concernées par différentes législations. Avec la publication le 16 novembre 2016 du décret d'application de la **Loi Jardé** votée en mars 2012 (décret 2016-1537), celle-ci s'applique désormais dans son intégralité.

Dorénavant, les Comités de Protection des Personnes (CPP) sont consultés pour tout type de dossier, **interventionnel ou non interventionnel,** du moment que le projet porte sur une **recherche impliquant la personne humaine**. Les recherches impliquant la personne humaine et relevant de la loi Jardé sont classées en 3 catégories en fonction du risque encouru :

- **La catégorie 1** concerne les recherches à **risque** et impose un avis du CPP et une autorisation de l'ANSM (L'Agence nationale de sécurité du médicament et des produits de santé).
- **La catégorie 2** concerne les recherches à **risques et contraintes minimes** (hors médicament) et ne demande que l'avis du CPP.
- **La catégorie 3** correspond aux recherches autrefois appelées observationnelles et, désormais, appelées **non interventionnelles** qui requièrent un avis CPP. On y trouve des études prospectives sur données, des études faisant appel à des questionnaires dans la mesure où ces études ne modifient pas la prise en charge du sujet.

Pour alléger les formalités liées aux traitements de données réalisés dans les recherches dans le domaine de la santé, la CNIL a adopté plusieurs **méthodologies de référence (« MR »)** adaptées aux recherches sur les données de la santé.

Afin de vous aider à déterminer quelle réglementation s'applique à votre projet de recherche, la DAJ de l'IRD met à votre disposition un logigramme d'aide à la qualification.
Vous pouvez contacter votre DPO qui vous indiquera les démarches à suivre.

Dans tous les cas, les projets de recherche en santé doivent :

- être portés par un **promoteur** qui en assure la gestion, veille au respect des bonnes pratiques garantissant l'intégrité de l'étude et vérifie que le financement est acquis ;
- recevoir une autorisation de la Commissions nationale informatique et liberté (CNIL) concernant le **traitement des données à caractère personnel** des personnes impliquées (ou respecter une méthodologie de référence) ;
- **informer les personnes sollicitées** pour participer à une étude sur l'objectif de la recherche, sa méthodologie, les bénéfices attendus, les contraintes et les risques prévisibles, le droit de refuser de participer et celui de retirer son consentement à tout moment ;
- **recueillir leur accord de participation à l'étude** et s'assurer qu'elles ont bien compris les informations données. En fonction de la catégorie de l'étude, cet accord peut être un consentement (écrit, express) ou une non-opposition ;