La science pour la santé
From science to health

Recherche en santé et protection des données personnelles : la nouvelle donne

DESC COCHIN

Frédérique LESAULNIER
Déléguée à la protection des données

Le RGPD : Règlement Général sur la Protection des Données

En Anglais, GDPR pour General Data Protection Régulation

Texte de référence en matière de protection des données pour l'ensemble des Etats de L'UE et au-delà

Date clé :

- Directement applicable dans tous les Etats membres de l'UE à partir du 25 mai 2018

Une nécessaire articulation avec le droit national

Un règlement à mi-chemin entre un règlement et une directive

- ✓ D'importantes marges de manœuvre laissées aux EM (maintien ou introduction de **spécificités nationales** pour certains types de traitements)
  - Nécessité d'adapter la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2016 et 2018
  - Nécessité d'articuler le RGPD avec les autres dispositions de l'UE et le droit national applicables à la recherche :
    - Au niveau européen
    - Règlement européen UE 2014/536 du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain
    - Au niveau national
    - Loi du 26 janvier 2016 de modernisation de notre système de santé
    - Règlementation applicable aux recherches impliquant la personne humaine (Loi du 5 mars 2012 et Ordonnance du 16 juin 2016)

Une évolution plus qu'une révolution dans la régulation

Un **cadre juridique riche et ancien** qui définit les conditions d'utilisation d'accès et d'utilisation des données à caractère personnel et en assure la protection

Il traduit le **caractère sensible** des **données de santé**

Ce cadre présentait déjà une **dimension européenne** :

- La Convention 108 du Conseil de l'Europe du 28 janvier 1981
- La **Directive européenne** 95/46/CE **du 24 octobre 1995** relative à la protection des personnes physiques à l'égard du traitement des données personnelles

La protection des données personnelles avant le 25 mai 2018 en bref

- ✓ La législation informatique et libertés (LIL) encadre les « traitements de données à caractère personnel » avec deux types d'obligations de valeurs égales :
  - Des **obligations de «fond »** qui doivent aujourd'hui être prises en compte dès la conception du projet
  - Une **obligation de « procédure »** (formalités administratives) préalable à la mise en œuvre d'un traitement qui impactent le planning du projet
- ✓ Leur respect engageait la **responsabilité pénale et administrative** du seul **responsable de traitement** qui **pouvait** désigner un Correspondant informatique et libertés (CIL)
- ✓ Des sanctions relativement faibles et peu appliquées

Le RGPD : Objectifs, calendrier et modalités d'application

Objectifs

- ✓ **Harmoniser les règles en matière de protection des données** et promouvoir un marché unique et cohérent au sein de l'UE (Viviane Reding, « one continent, one law »)
- ✓ **Remplacer** la Directive européenne 95/46/CE et prendre en compte l'évolution de l'environnement numérique
- ✓ **Renforcer et moderniser les droits des personnes** sur leurs données personnelles
- ✓ **Diminuer les lourdeurs administratives** et responsabiliser les acteurs
- ✓ Renforcer le cadre institutionnel, le rôle des Autorités de protection des données et leur coopération
- ✓ Faire prévaloir le modèle européen de protection des données face à la mondialisation et **faciliter les flux de données**

Champ d'application territorial du RGPD

- **Le RGPD** s'applique dans deux cas :

- Le responsable du traitement ou du sous-traitant est établi (d'une façon stable) sur le territoire de l'Union que le traitement ait lieu ou non sur le territoire de l'Union ;
- Le traitement cible des résidents européens :

- **Les règles nationales prise en application du RGPD**, dans le cadre des marges de manœuvre laissées aux États membres (chapitre IX applicable à la recherche), s'appliquent dès lors qu'une personne concernée par le traitement **réside en France**, y compris lorsque le responsable de traitement n'est pas établi en France » (art. 5-1)

RGPD : La donnée à caractère personnel : une définition large qui ne change pas fondamentalement

« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art. 4.1)

Le Règlement n'est pas applicable aux données anonymes, qu'elles le soient initialement ou qu'il s'agisse de données à caractère personnel qui ont donné lieu à une anonymisation.

La possibilité d'identifier les personnes s'apprécie au regard des moyens « **raisonnablement** susceptibles d'être utilisés **par le responsable de traitement ou par toute autre personne** ».

La partie de l'image avec l'ID de relation rId2 n'a pas été trouvé dans le fichier.

RGPD : Pseudonymisation : une définition nouvelle

« Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

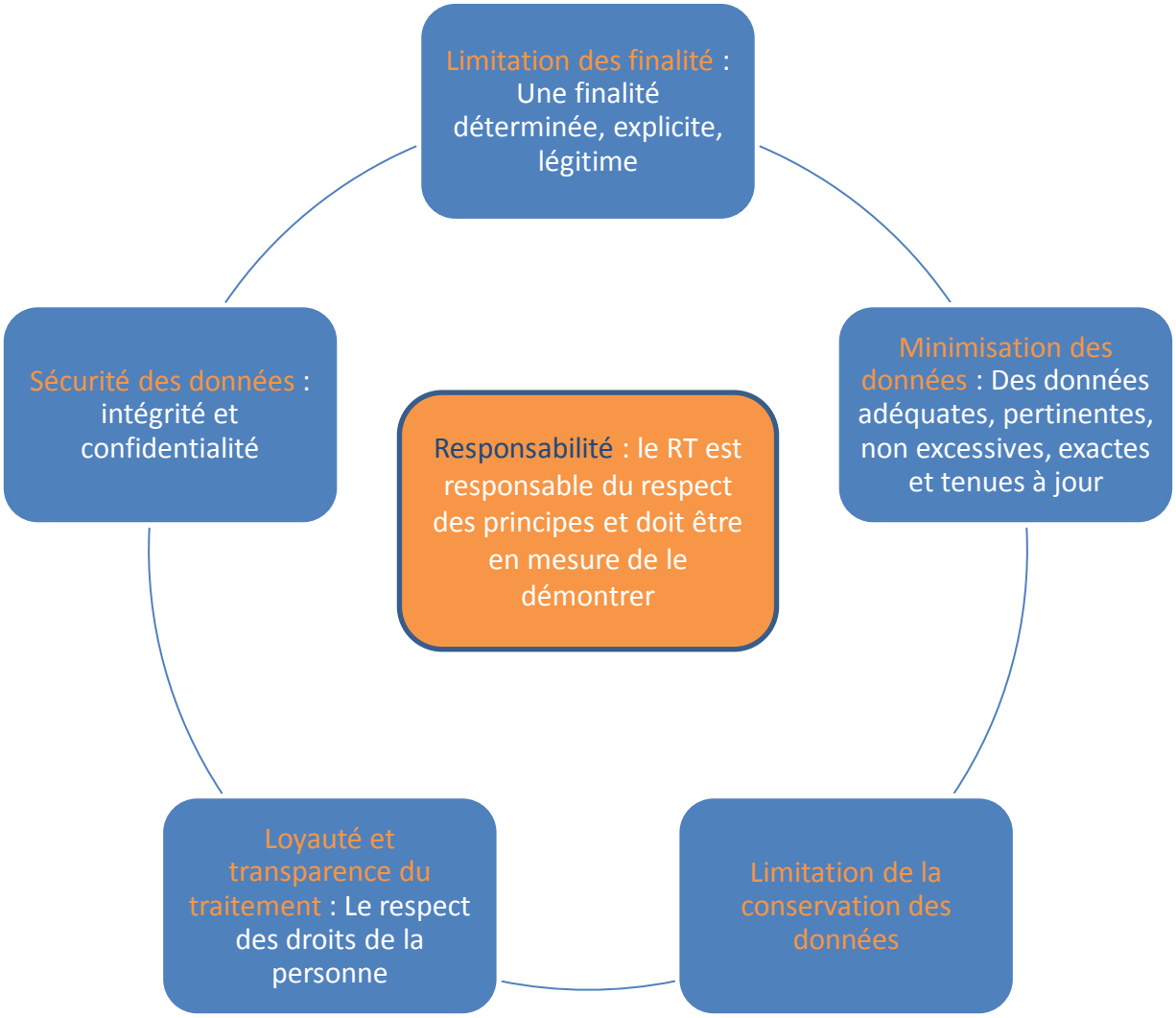
- **Cette définition couvre différentes techniques couramment utilisées en matière de recherche en santé**:

• le recours à une table de correspondance entre le jeu de données pseudonymes et les données d'identité conservées séparément, classiquement utilisée dans les essais cliniques ;

• les fonctions de hachage utilisées avec un secret qui permettent de chaîner des données relatives à un individu dans le temps sans permettre de l'identifier

La partie de l'image avec l'ID de relation rId2 n'a pas été trouvé dans le fichier.

Les principes fondamentaux de la protection des données personnelles reconduits et renforcés



RGPD : Fondements légaux pour les traitements reconduits : art. 6

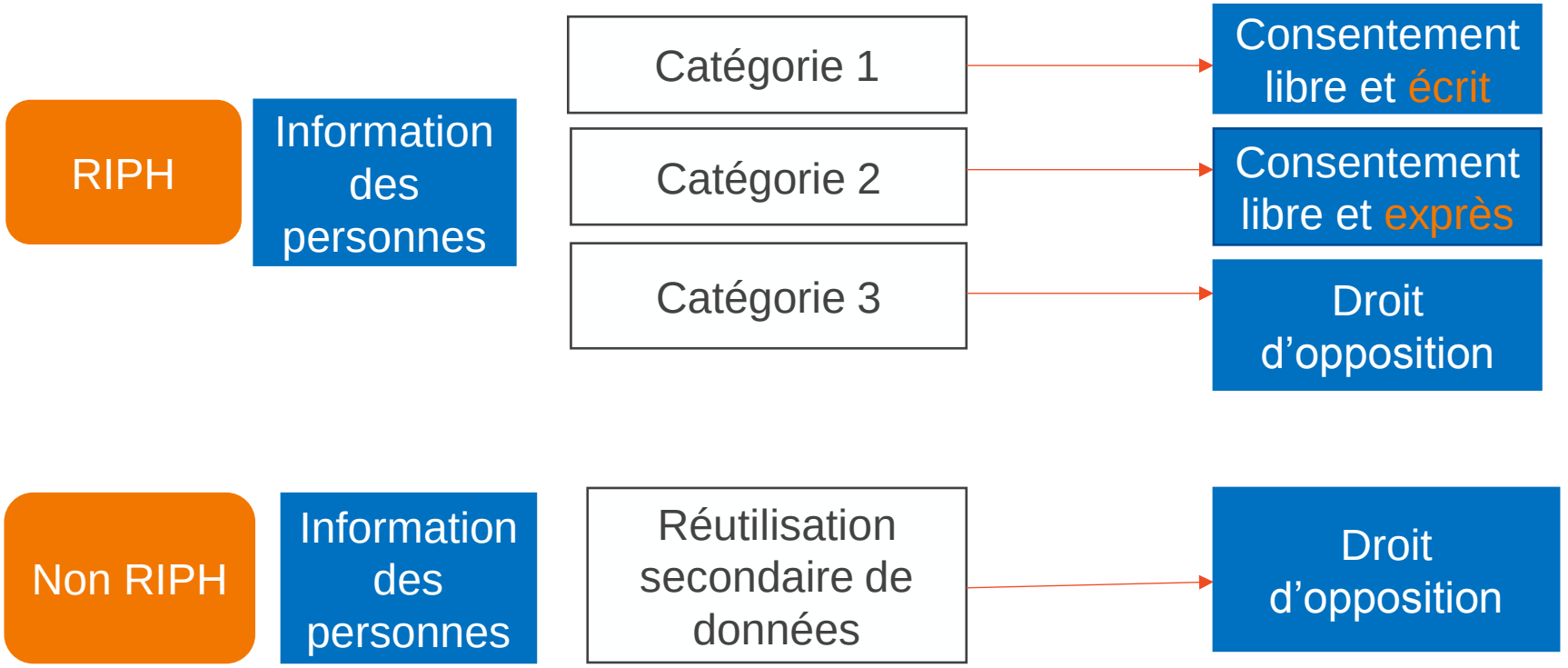
- Pour être licite, le traitement doit reposer sur un fondement
- L'article 6 du RGPD liste les bases juridiques permettant de considérer que le traitement des données est licite.

Le responsable de traitement doit s'appuyer sur l'un de ces fondements pour réaliser sa recherche et la mentionner dans la note d'information.

- **Consentement** au traitement par la personne concernée portant sur une ou plusieurs finalités spécifiques
- Nécessité pour l'exécution d'un contrat ou de mesures précontractuelles
- Nécessité pour le respect d'une obligation légale
- Nécessité pour la sauvegarde d'intérêts vitaux
- Nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
- Nécessité aux fins des **intérêts légitimes du RT** ou d'un tiers (exclu pour les traitements effectués par les autorités publiques dans le cadre de l'exercice de leurs missions)

- A articuler avec **l'article 9.2 (j)** du RGPD, qui mentionne la nécessité de traiter les données à des fins de recherche scientifique.

Impact de la qualification réglementaire sur les droits des personnes



La partie de l'image avec l'ID de relation rId2 n'a pas été trouvé dans le fichier.

Un changement de paradigme : vers une responsabilisation accrue des acteurs du traitement (RT et ST)

D'une logique de formalités préalables à une logique de mise en « conformité » dynamique, continue, effective et démontrable et de « responsabilité »

- La responsabilité devient une **condition de licéité du traitement** : la charge de la preuve de la conformité des traitements au RGPD incombe au RT
- Nécessaire développement de **politiques d'*accountability*** qui passent par la mise en œuvre et l'actualisation de **mesures techniques et organisationnelles** adéquates pour garantir la conformité
- De nombreuses **obligations nouvelles** qui pèsent sur les acteurs dont le **non-respect est lourdement sanctionné**

Les obligations nouvelles qui pèsent sur les acteurs

- Désigner un **Délégué à la Protection des Données** (DPO)

- Tenir un **registre** généralisé à l'ensemble des traitements

- Mener des **analyses d'impact** sur la vie privée et les libertés (PIA) pour les traitements qui présentent un risque élevé pour les droits et libertés des personnes

- Maintien d'un régime d'autorisation pour la recherche en **santé** (LIL, chapitre IX)
- **Consulter** la CNIL pour les traitements présentant un risque élevé pour les droits et libertés des personnes
- Notifier les **failles de sécurité** dans les 72 heures à compter de leur découverte

- Prendre en compte la protection des données dès la conception et par default

Une responsabilisation accrue de tous les acteurs du traitement (RT et ST)

- Possibilité nouvelle de **responsabilités conjointes** du traitement (art. 26)
- Introduction de **nouvelles responsabilités** pour les « **sous-traitants »** (art. 28) et un **principe de responsabilité conjointe** dans certains cas : la sécurité notamment (art. 32)
- **Encadrement plus strict des relations avec les partenaires et sous-traitants** (art. 28) qui devront aussi être conformes au RGPD.
- Nécessité d'établir la chaîne de responsabilité et documenter : Les **contrats** ou **conventions** devront préciser les nouvelles obligations et responsabilités et définir les obligations respectives

Les obligations nouvelles qui pèsent sur les acteurs

Développements d'outils pour apporter une preuve de la conformité

- La promotion des **codes de conduite** par secteur d'activité (Article 40)

- Des mécanismes de **certification** et de **labellisation** proposées par le Comité européen à la protection des données (futur ex G29) et les institutions de l'UE (Article 42)

RGPD : renforcement des droits des personnes

- **Renforcement des obligations de transparence et d'information**
  - Les informations sur le traitement doivent être concises, transparentes, compréhensibles et aisément accessibles (spécialement à l'égard des enfants)
  - Des informations plus nombreuses à fournir par le responsable du traitement
  - Une information préalable de spécifique à chaque projet
  - L'information peut être accompagnée d'icônes standardisées
  - Dérogations en cas de collecte indirecte des données : la personne dispose déjà des informations, information impossible ou qui exigerait des efforts disproportionnés en particulier pour les traitements à des fins scientifiques ou historiques ou à des fins scientifiques

RGPD : renforcement des droits des personnes

- Droit d'**accès** et de **rectification**
- **Droit à l'effacement** (droit à l'oubli numérique) (CJUE arrêt Google Spain 13 mai 2014) : Une exception en matière de recherche scientifique lorsque « l'exercice de ce droit risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement » (qui trouve un écho dans le CSP pour les RIPH)
- Droit à la **portabilité** des données (pas systématiquement applicable en matière de recherche)
- Droit à la **limitation** du traitement
- Droit à être informé d'une **violation** des données en cas de risques élevés pour les intéressés
- Une protection des mineurs

Impact de la loi du 6 janvier 1978 modifiée en 2018 sur la recherche en santé

Maintien d'une procédure d'autorisation des traitements à des fins de recherche, d'étude et d'évaluation dans le domaine de la santé

- La section 3 du chapitre III du titre II de la LIL (ancien chapitre IX) régit désormais l'ensemble des **traitements de données à caractère personnel dans le domaine de la santé**.
- Pour la recherche en santé présentant une **finalité d'intérêt public**, application cumulative des sections I (dispositions générales) et II (dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé).
- **La CNIL autorise** le traitement **après avis** : (art. 76)

1° Du **Comité de protection des personnes** (CPP) pour les RIPH;

2° Du **Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé** (CEREES), pour les études ou à des évaluations ainsi qu'à des recherches hors RIPH.

3° De **l'INDS sur le caractère d'intérêt public** que présente la recherche, l'étude ou l'évaluation (pas systématique).

La demande d'autorisation est **réputée acceptée** en cas de silence de la CNIL (condition : « l'avis ou les avis rendus préalablement soient « expressément favorables ») (art. 66)

- Alignement des règles d'utilisation du NIR-INS sur le NIR pour les traitements mis en place à des fins de recherche en santé

Recherche impliquant la personne humaine

- **Définition RIPH** (CSP, art. L.1121-1) :
  1. Recherches **organisées** et **pratiquées sur l'être humain**
  2. En vue du **développement des connaissances biologiques ou médicales**
- **Trois catégories** de RIPH:
  1. **Les recherches interventionnelles** qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle (intègre les essais cliniques de médicaments jusqu'à l'entrée en application du RE n°536/2014)
  2. **Les recherches interventionnelles ne comportent que des risques et des contraintes minimes** (liste fixée par arrêté du 12 avril 2018)
  3. **Les recherches non interventionnelles** qui ne comportent aucun risque ni contrainte dans lesquelles tous les actes sont pratiqués et les produits utilisés de manière habituelle (liste fixée par arrêté du 12 avril 2018)
- Pour ces trois catégories, **l'avis favorable d'un CPP est nécessaire** (CSP, art. L. 1123-6)

Recherche n’impliquant pas la personne humaine

Ne sont pas des recherches impliquant la personne humaine :

- Les recherches ayant une finalité d’intérêt public de recherche, d’étude ou d’évaluation dans le domaine de la santé **conduites exclusivement à partir de l’utilisation secondaire de données et d'échantillons déjà collectés** (études rétrospectives)
- Les recherches prospectives qui n'entrent pas dans le champ de « Jardé" parce qu'elle ne sont **pas "organisées et pratiquées sur l’être humain en vue du développement des connaissances biologiques ou médicales**" (ex : études menées en sciences humaines et sociales)
- Les dossiers relatifs à ces études sont déposés auprès du secrétariat de l’INDS et soumis à l’avis du CEREES

De la procédure d'autorisation à l'engagement de conformité à une MR

<table>
<tr><th>Types de recherche</th><th colspan="3">Recherche impliquant la personne humaine</th><th colspan="2">Recherche n'impliquant pas la personne humaine</th></tr>
<tr><td rowspan="2"></td><td>Catégorie 1
Recherche interventionnelle</td><td>Catégorie 2
Recherche interventionnelles à risques et contraintes minimes</td><td>Catégorie 3
Recherche non interventionnelle</td><td>Etudes rétrospectives : recherche, étude ou évaluation conduite exclusivement à partir de l'utilisation secondaire de données et d'échantillons déjà collectés</td><td>Recherches prospectives
« organisées et pratiquées sur l'être humain » hors finalités RIPH</td></tr>
<tr><td colspan="3">Avis CPP dans tous les cas</td></tr>
<tr><td>Champ d'application MR</td><td colspan="2">MR001
Consentement écrit ou exprès requis</td><td>MR003
Information et non opposition

MR001 si examen des caractéristiques génétiques</td><td colspan="2">MR004
Information et non opposition
Aménagements information individuelle
Pas d'avis CEREES</td></tr>
<tr><td>En cas de non-conformité avec les MR</td><td colspan="3">Avis CPP + autorisation CNIL
Saisine INDS possible sur intérêt public</td><td colspan="2">Dépôt du dossier auprès de l'INDS
Avis CEREES + Autorisation CNIL
Saisine INDS possible sur intérêt public</td></tr>
</table>

Merci de votre écoute

dpo@inserm.fr

©Inser

La partie de l'image avec l'ID de relation rId2 n'a pas été trouvé dans le fichier.