

LA PROTECTION DES DONNÉES PERSONNELLES

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Présenté par

Simon DALMAZ

Chargé d'affaires juridiques délégué à la protection des données

INTRODUCTION

- ▶ Faisant suite et venant compléter la Loi Informatique et Libertés de 1978, le Règlement Général sur la Protection des Données personnelles (RGPD) est entré en vigueur le 25 mai 2018.
- ▶ Le RGPD renforce et accroît les droits des personnes sur leurs données personnelles et augmente la responsabilité des organismes traitant ces données. Ces organismes sont appelés « responsable de traitement ».
- ▶ Un des changements majeurs consiste en la suppression de la plupart des obligations déclaratives auprès de la CNIL (déclarations, autorisations) au profit d'une logique **d'auto-responsabilité**. Les responsables de traitements devront donc veiller eux même au respect de la réglementation tout au long du cycle de vie de la donnée (collecte, traitement, archivage, suppression).

DÉFINITIONS

- ▶ **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «**personne concernée**») ; est réputée être une «personne identifiable» une personne qui peut être identifiée, notamment par référence à un identifiant, un numéro d'identification, des données de localisation, ou à un élément spécifique propre à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- ▶ **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, la structuration, la modification, la consultation, la communication, la diffusion, l'effacement ou la destruction.
- ▶ **Responsable du traitement** : la personne physique ou morale qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Il s'agit dans tous les cas du Directeur de laboratoire.
- ▶ **Sous-traitant** : la personne physique ou morale, qui traite des données à caractère personnel pour le compte du responsable du traitement (sous-traitant pour les sondages...). Nous sommes responsable des actes du sous-traitant donc prévoir une convention.
- ▶ **Destinataire** : la personne, qui reçoit des données à caractère personnel dans le cadre de la recherche, qu'il s'agisse ou non d'un tiers.

LES TRAITEMENTS DE DONNÉES SENSIBLES

► **L'article 9 du RGPD en donne la définition et pose l'interdiction :**

Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données de santé, génétiques, biométriques ou encore concernant la vie ou l'orientation sexuelle d'une personne physique sont interdits.

► **L'article 9.2 prévoit quelques exceptions à cette interdiction :**

- La personne concernée a donné son **consentement** (rétractable à tout moment)
- Le traitement est nécessaire pour des motifs **d'intérêt public** dans le domaine de la santé publique
- Le traitement est nécessaire **à des fins de recherche scientifique** ou historique ou à des fins statistiques.

LES PRINCIPES CLÉS DE TOUT TRAITEMENT

► **Licite, loyal, transparent :**

Les données doivent être traitées de manière licite, loyale et transparentes au regard de la personne concernée (mentions d'informations claires et précises) ;

► **Le principe de finalité du traitement :**

Les données personnelles ne peuvent être recueillies et traitées que pour une finalité déterminée explicite et légitime.

La finalité doit être déterminée avant la collecte des données. Pas de collecte « au cas où ».

Lesdites données ne pourront pas être réutilisées ultérieurement pour une autre recherche sans obtenir le consentement écrit des personnes concernées. Les données peuvent être réutilisées sous certaines conditions :

Données anonymes

Faire mention d'une réutilisation des données dans le formulaire de consentement

► **Le principe de proportionnalité et de minimisation :**

Seules les informations adéquates, pertinentes et nécessaires à la finalité du traitement peuvent faire l'objet du traitement. Inutile de collecter des informations qui ne sont pas indispensables à la réalisation de l'étude. Si possible, se passer de données personnelles.

► **Le principe d'une durée de conservation limitée des données :**

Une durée de conservation doit être établie en fonction de la finalité de chaque traitement. Il peut y avoir différentes durées pour différentes données au sein d'un même traitement. Une fois le traitement réalisé et les résultats obtenus, inutile de conserver les données personnelles (**anonymisez vos données**). Seuls les formulaires de consentement et les données anonymes peuvent être conservés plus longtemps pour raisons de recherche (sauf obligations légales de conservation ou d'archivage).

► **Le principe de sécurité et de confidentialité :**

Les données collectées ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs missions (mentionnées dans le formulaire de consentement).

Il est nécessaire de prendre toutes les mesures de protection nécessaire, physiques et logicielles, pour en garantir la confidentialité et éviter toute divulgation d'informations volontaires ou involontaires.

Plus les données sont sensibles, plus la sécurité et la confidentialité doit être importante.

UN STOCKAGE SÉCURISÉ

Il est nécessaire de respecter certaines précautions élémentaires en termes de sécurité :

- ▶ **Tenir secrets ses mots de passe (BIOS, SESSION, DOSSIER, FICHER)** (ex. : ne pas les noter sur un post-it, ne pas les communiquer à un proche ou un collègue, choisir un mot de passe complexe.) ;
- ▶ **Utiliser des antivirus** mis à jour et **installer un « pare-feu »** (firewall) logiciel ;
- ▶ **Etre prudent vis-à-vis des contenus extérieurs**, notamment les courriels (contact inconnu, tournures inhabituelles, etc.), une PJ, un lien de téléchargement sur un site web, etc. En cas de doute, ne cliquez pas ou n'ouvrez pas le document. Attention aux clés USB qui ne vous appartiennent pas. Ne jamais les insérer dans votre ordinateur.
- ▶ **Prévoir une procédure de verrouillage automatique de session** et verrouiller son ordinateur dès que l'on quitte son poste de travail ;
- ▶ **Enregistrer régulièrement vos travaux** pour éviter toute perte de données (sur un support sécurisé) ;
- ▶ **Ne pas stocker les données collectées sur des matériels non sécurisés** ; prévoir des moyens de chiffrement du matériel (logiciels); protection de fichiers par mot de passe.... Evitez les supports de stockage mobiles.

L'INFORMATION DES PERSONNES (MENTIONS LÉGALES)

► Le principe du respect des droits des personnes :

L'article 13 du RGPD exige que soient communiquées les informations suivantes auprès de la personne concernée :

- Les coordonnées du **responsable de traitement** ;
- Les coordonnées du **délégué à la protection des données** (ou de la personne en charge du traitement) ;
- La ou **les finalités** du traitement auquel sont destinées les données personnelles ;
- La **base juridique du traitement** (consentement de la personne concernée, le respect d'une obligation légale) ;
- **Les destinataires** des données ou catégories de destinataires y compris les partenaires ;
L'existence d'un transfert de données vers un pays tiers (CE décisions d'adéquation) ;
- **La durée de conservation** des données ou, lorsque cela n'est pas possible, les critères permettant de déterminer cette durée ;
- L'existence du **droit d'accès, de rectification, d'opposition ou de suppression** des données de la personne concernée avec la mention d'une adresse mail (postale ou téléphone selon la population visée) permettant d'exercer ces droits ;
- Lorsque le traitement est fondé sur le consentement de la personne, l'existence du **droit de retirer son consentement** à tout moment (retrait de la recherche et arrêt de traitement des données déjà collectées) ;
- Le droit d'introduire **une réclamation auprès de la CNIL**

LE FORMULAIRE DE CONSENTEMENT (ET LA NOTICE D'INFORMATION)

Cette recherche est réalisée dans le cadre de **XXXXX** sous la direction de **XXXXX** (*Nom du responsable scientifique et du Laboratoire et catégories de personnes habilitées*).

Cette recherche a pour but de **XXXXX** (*Finalité et avantages dans un vocabulaire à la portée de tous*)

Votre participation à cette recherche repose sur le **volontariat** et n'implique aucun risque ou inconfort pour vous.

Pour les besoins de cette recherche, vous serez amené à **XXXXX** (*lister ce que le participant devra faire, réaliser...*)

La participation à cette recherche est d'environ **XXXXX** (*durée totale et nombre de participation, entretiens*)

Aucune information personnelle ne sera diffusée et toutes les données recueillies seront utilisées aux seules fins de cette recherche et resteront strictement confidentielles. Les résultats publiables de cette recherche seront anonymes. Seuls le(s) Responsable(s) scientifique(s) et les chercheurs y auront accès.

Vous avez le droit de refuser de participer à cette recherche ou de retirer votre consentement à tout moment sans vous justifier et sans encourir aucune responsabilité ni aucun préjudice de ce fait.

Conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée et au Règlement européen (UE) 2016/679 du 25 mai 2018, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier ou supprimer ainsi que poser des questions au sujet de la recherche en tout temps en communiquant avec le Responsable scientifique du projet en contactant :

XXXXX (*Nom, Prénom, Laboratoire, adresse, Mail et téléphone*)

En signant ce formulaire, vous certifiez que vous avez lu et compris les renseignements ci-dessus et qu'on vous a avisé que vous étiez libre d'annuler votre consentement ou de vous retirer de cette recherche en tout temps, sans préjudice.

Je soussigné(e) : (NOM, Prénom)

Confirme avoir lu et compris les renseignements ci-dessus et consens librement à participer à cette recherche. Je comprends les implications de cette recherche, à laquelle j'accepte de participer.

Signature :

LE PROTOCOLE DE RECHERCHE (1/4)

DESCRIPTION DU PROJET

Contexte de la recherche et intérêts scientifiques / Objectifs / Hypothèses générales

METHODOLOGIE

► PARTICIPANTS

- **Nombre exact de participants :**
- **Population cible :**
- **Mode et source de recrutement :** par annonces, par affichage, par listings, etc...
- **Lieu de recrutement :** précisez le lieu de recrutement envisagé ou critères qui orienteront le choix du lieu
- **Critères de sélection :** précisez les critères de sélection des participants en fonction de vos objectifs de recherches. Ces critères peuvent porter sur la tranche d'âge, le milieu socioculturel, niveau d'éducation, la nationalité, l'implication dans le processus étudié, etc.
- **Critères de non inclusion :** précisez les critères de non inclusion des participants en fonction de vos objectifs de recherches. Ces critères interviennent une fois que vous avez sélectionné vos participants, c'est-à-dire qu'ils conduiront à ne pas inclure dans votre protocole certains des participants sélectionnés. Ces critères peuvent porter sur des troubles visuels, auditifs, neurologiques, des conduites addictives, etc.
- **Détailler les supports utilisés pour le recueil de données** (exemple : description des questionnaires, grilles d'entretien, exploitation de base de données...)
- **Indemnisation éventuelle des sujets** (compensation pour frais ou indemnité de pénibilité, pas de contrepartie financière pour faciliter le recrutement)

LE PROTOCOLE DE RECHERCHE (2/4)

► METHODE

- **Description du protocole** : Type d'étude (tâches, questionnaires, etc...).
- **Matériel utilisé** (enregistrement audio, vidéo, images ...)
- **Lieu ou l'étude va être conduite** :
- **Calendrier des évaluations ou observations** début et fin (en mois et année), nombre de sessions d'évaluation sur un participant, durée de l'évaluation sur un participant.
- **Durée de l'étude par participant** ce point correspond à la durée du recueil des données
- **Analyse des données** : Description de l'analyse des données (quantitative et qualitative)

► BENEFICES ET RISQUES PREVISIBLES ET CONNUS POUR LA SANTE PHYSIQUE ET MENTALE

- Présentez les **bénéfices de votre étude**. Il peut s'agir de bénéfices en termes d'avancées scientifiques, d'amélioration de la qualité de vie des participants, de leur estime de soi...
- Présentez les **risques de votre étude**. Il peut s'agir de risques en termes d'effets secondaires (selon la finalité et la thématique de la recherche), d'efforts, questions personnelles susceptibles de troubler le participant...

LE PROTOCOLE DE RECHERCHE (3/4)

► CONFIDENTIALITE

- Procédé d'anonymisation :

La notion d'anonymisation des données est plus large que la simple dissimulation du nom. Elle implique l'impossibilité de faire correspondre l'identité des sujets aux données, même par des moyens indirects.

Toutefois, il faut distinguer deux cas :

Anonymisation : par défaut pour les études quantitatives - Le protocole est tel que les données traitées sont anonymes ou rendues anonymes grâce à l'usage de numéros aléatoires. Elles ne permettent pas d'identifier même indirectement la personne de quelque manière que ce soit ; ce ne sont donc plus des données à caractère personnel et il n'existe pas de table de correspondance entre l'identité de chaque personne et un numéro aléatoire renvoyant à une série de données individuelles. Cette solution est la plus sûre mais ne permet pas de faire une étude nécessitant un suivi des participants sur la durée (plusieurs entretiens, questionnaires successifs...)

Pseudonymisation : Si votre recherche nécessite de recontacter les personnes concernées - Dans ce cas il existe une table de correspondance entre chaque personne et les numéros aléatoires identifiant la série de données correspondante (2 tableaux Excel protégés par un mot de passe différent et stockés sur des supports différents).

Ici, l'anonymat strict ne peut pas être garanti (personnes identifiées ou identifiables dans les documents, même partiellement ou temporairement). Une fois les résultats obtenus, supprimer la table de correspondance rendra les données parfaitement anonymes.

- Personnes ayant accès aux données :

Vous devez préciser les personnes qui auront accès aux données : responsable scientifique, chercheur(s), etc.

LE PROTOCOLE DE RECHERCHE (4/4)

▶ TRAITEMENT DES DONNEES

- **Type de données traitées (santé, Etat civil, adresses, descriptions physiques, captation audio, vidéo...)**

- **Durée de conservation :**

Supprimer les données personnelles une fois exploitées dans la mesure où elles ne seront plus nécessaires par la suite.

Supprimer s'il y a lieu la table de correspondance lorsqu'il n'est plus utile de contacter les personnes concernées.

- **Lieu de stockage :**

Préciser où seront stockées les données nominatives (la liste numéros aléatoires - nom participant), les consentements et lettres d'information. Préciser où seront stockées les données non nominatives (réponses aux questionnaires, données socio démographique, résultats à l'expérience). Dire qui s'occupe de la saisie des données, qui a accès aux données...

En somme, décrire les flux de donnée.

- **Modalités de destruction/retrait à la demande du participant (droit de retrait du consentement et droit de suppression)**

LE COMITE DE PROTECTION DES PERSONNES (CPP)

► La mission des CPP :

Les Comités de Protection des Personnes (CPP) sont chargés d'émettre un **avis préalable sur les conditions de validité de toute recherche impliquant la personne humaine**, au regard des critères définis par l'article L.1123-7 du Code de la Santé Publique (CSP). Cet avis est contraignant, s'il n'est pas favorable, il interdit la mise en place de la recherche

Les termes de "**recherche impliquant la personne humaine**" désignent, tout essai ou expérimentation organisé et pratiqué sur l'être humain, en vue du développement des connaissances biologiques ou médicales.

Les CPP se prononcent sur les conditions dans lesquelles le promoteur de la recherche (CHU) assure la protection des personnes et notamment des participants, sur le bien-fondé et la pertinence du projet de recherche et sur sa qualité méthodologique (protocole, information préalable, recueil du consentement, période d'exclusion, délai de réflexion...). Toute modification du protocole devra aussi faire l'objet d'un avis favorable du C.P.P.

La personne physique ou morale qui prend l'initiative d'une recherche impliquant la personne humaine est dénommée "**promoteur**". La ou les personnes physiques qui dirigent et surveillent la réalisation de la recherche sur un lieu sont dénommées "**investigateurs**".

DISTINCTION RECHERCHE IMPLIQUANT LA PERSONNE HUMAINE / N'IMPLIQUANT PAS LA PERSONNE HUMAINE

Article R.1121-1 CSP

I. – **Sont des recherches impliquant la personne humaine**, les recherches organisées et pratiquées sur des personnes volontaires saines ou malades, en vue du développement des connaissances biologiques ou médicales qui visent à évaluer :

1° Les mécanismes de fonctionnement de l'organisme humain, normal ou pathologique ;

2° L'efficacité et la sécurité de la réalisation d'actes ou de l'utilisation ou de l'administration de produits dans un but de diagnostic, de traitement ou de prévention d'états pathologiques.

II. – 1° **Ne sont pas des recherches impliquant la personne humaine**, les recherches qui, bien qu'organisées et pratiquées sur des personnes saines ou malades, n'ont pas pour finalités celles mentionnées au I, et qui visent :

a) Pour les produits cosmétiques, à évaluer leur capacité à nettoyer, parfumer, modifier l'aspect, protéger, maintenir en bon état le corps humain ou corriger les odeurs corporelles ;

b) A effectuer des enquêtes de satisfaction du consommateur pour des produits cosmétiques ou alimentaires ;

c) A effectuer toute autre enquête de satisfaction auprès des patients ;

d) A réaliser des expérimentations en sciences humaines et sociales dans le domaine de la santé (MR-04).

2° Ne sont pas des recherches impliquant la personne humaine, les recherches qui ne sont pas organisées ni pratiquées sur des personnes saines ou malades et n'ont pas pour finalités celles mentionnées au I, et qui visent à évaluer des modalités d'exercice des professionnels de santé ou des pratiques d'enseignement dans le domaine de la santé.

LES MÉTHODOLOGIES DE RÉFÉRENCE

Vous ne pouvez pas, en tant que doctorant ou étudiant, réaliser une formalité auprès de la CNIL en votre nom propre (engagement de conformité à une MR ou demande d'autorisation « recherche »). C'est à votre université ou à l'établissement de soin auquel vous êtes rattaché qui devra effectuer cette démarche, en sa qualité de responsable de traitement.

L'engagement de conformité à une MR n'est pas à réaliser pour chaque recherche : il vaut pour l'ensemble des traitements d'un même responsable de traitement entrant dans le champ de la MR

Pour les recherches n'impliquant pas la personne humaine (RNIPH) et multicentrique: Si la recherche est conforme à la MR-004, MR 005 ou MR 006, les informations relatives à la recherche menée dans le cadre de ces MR devront faire l'objet d'un enregistrement en ligne dans un répertoire public, dont l'INDS est en charge.

LES MÉTHODOLOGIES DE RÉFÉRENCE

- ▶ Méthodologie de référence MR-001 : recherches dans le domaine de la santé avec recueil du consentement
- ▶ Méthodologie de référence MR-002 : études non interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro
- ▶ **Méthodologie de référence MR-003 : recherches impliquant la personne humaine dans le domaine de la santé sans recueil du consentement**
- ▶ **Méthodologie de référence MR-004 : recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé**
- ▶ Méthodologie de référence MR-005 : études nécessitant l'accès aux données du PMSI et/ou des RPU par les établissements de santé et les fédérations hospitalières
- ▶ Méthodologie de référence MR-006 : études nécessitant l'accès aux données du PMSI par les industriels de santé

LES MÉTHODOLOGIES DE RÉFÉRENCE

► **Méthodologie de référence MR-003 : recherches impliquant la personne humaine dans le domaine de la santé sans recueil du consentement**

La méthodologie de référence MR-003 encadre les traitements comprenant des données de santé et présentant un caractère d'intérêt public, réalisés dans le cadre de recherches impliquant la personne humaine pour lesquelles la personne concernée ne s'oppose pas à participer après avoir été informée. Il s'agit plus précisément des recherches non interventionnelles et des essais cliniques de médicaments par grappe. L'information individuelle des patients est obligatoire. Le responsable de traitement s'engage à ne collecter que les données strictement nécessaires et pertinentes au regard des objectifs de la recherche.

► **Méthodologie de référence MR-004 : recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé (SHS dans le domaine de la santé)**

La méthodologie de référence MR-004 encadre les traitements de données à caractère personnel à des fins d'étude, évaluation ou recherche n'impliquant pas la personne humaine. Il s'agit plus précisément des études ne répondant pas à la définition d'une recherche impliquant la personne humaine, ainsi que les études portant sur la réutilisation de données. La recherche doit présenter un caractère d'intérêt public. Le responsable de traitement s'engage à ne collecter que les données strictement nécessaires et pertinentes au regard des objectifs de la recherche.

CPP ET MÉTHODOLOGIES DE RÉFÉRENCE

Quelle est la nature de votre recherche ? (2 options) :

- ▶ Soit il s'agit d'une **recherche impliquant la personne humaine (CPP)** il faut distinguer l'interventionnel et le non-interventionnel. Dans tous les cas vous devez vous rapprocher du CHU ou de l'établissement de santé concerné pour saisir le CPP.

Interventionnelle :

- **RIPH 1** : Les recherches interventionnelles qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle (médicament expérimental, dispositifs médicaux très invasifs);
- **RIPH 2** : Les recherches interventionnelles qui ne comportent que des risques et des contraintes minimales, dont la liste est fixée par arrêté du ministre chargé de la santé, après avis du directeur général de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) (soins courants (hors expérimental); dispositifs médicaux non ou peu invasifs)
- **Plus MR-01**

Non interventionnelle (observationnelle) :

- **RIPH 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.
 - **Plus MR-02 ou 03**
- ▶ Soit il s'agit d'une **recherche n'impliquant pas la personne humaine (CERNI OU MR-04/05/06)**

CPP ET MÉTHODOLOGIES DE RÉFÉRENCE

Recherche impliquant la personne humaine (avis favorable du CPP requis et MR)

Recherche interventionnelle
(RIPH 1)

Recherche interventionnelle à risques et
contraintes minimales (RIPH 2)

Recherche non interventionnelle
(RIPH 3)

Engagement de conformité à la
MR-001

Engagement de conformité à la MR-001

Engagement de conformité à la MR-
002 ou à la MR-003

Engagement de conformité à
la MR-004 (plus enregistrement à
l'INDS), MR-005 ou à la MR-006

+

+

+

+

Inscription au registre des
activités de traitement

Inscription au registre des activités de
traitement

Inscription au registre des activités de
traitement

Inscription au registre des activités
de traitement

Recherche n'impliquant pas la personne humaine (CERNI ou MR)