



Guide des bonnes pratiques liées aux données personnelles dans le domaine de la recherche (hors données de santé)

Janvier 2020

L'exploitation et le traitement de données personnelles poursuivant une finalité de recherche scientifique sont soumis aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le « RGPD ») ainsi qu'à celles de la loi « Informatique et libertés » (loi n° 78-17 du 6 janvier 1978 modifiée).

Le RGPD définit la recherche scientifique largement. Son considérant 159 indique ainsi que *« le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé »*.

Un cadre particulier est prévu pour ces traitements afin de concilier les spécificités de la recherche avec l'impératif de protection des données personnelles. La CNIL a publié en juin 2019 un guide *« Régime juridique applicable aux traitements poursuivant une finalité de recherche scientifique (hors santé) »*.

Ce guide s'adresse aux étudiants, élèves, enseignants, enseignants chercheurs, stagiaires, apprentis, vacataires et plus généralement toute personne entreprenant des travaux visant à recueillir des données à caractère personnel dans un but d'enseignement et de recherche. Il vise à constituer un ensemble de recommandations et de bonnes pratiques assurant le respect du traitement des données à caractère personnel dans un but d'enseignement et de recherches.

I - QU'EST-CE QU'UNE DONNEE PERSONNELLE ?

Les données personnelles sont toutes les informations relatives à une personne physique identifiée, ou qui peut être identifiée en croisant des données la concernant. Un numéro de sécurité sociale est une donnée personnelle. Un âge (« 13 ans », ou « 54 ans ») est aussi une donnée personnelle ; cette information semble banale et sans enjeu, elle permet pourtant d'identifier une personne si on la croise avec une adresse.

De nombreuses autres informations constituent également des données personnelles : le nom, le prénom, l'âge, le métier, une photo, l'adresse postale, l'adresse mail, le numéro de téléphone, la date de naissance, le numéro IP (*Internet Protocol*), tout numéro d'identification, par exemple le Numéro d'inscription au répertoire (le NIR, qu'on appelle usuellement le numéro de sécurité sociale), une empreinte digitale, des données de géolocalisation, et tous *« éléments spécifiques propres à son identité physique, physiologique, générique, psychique, économique, culturelle ou sociale »*. Une institution (organisation ou entreprise, association...) ne constituant pas une personne physique n'entre pas dans le champ du RGPD.

Le RGPD distingue les données sensibles qui font l'objet de mesures spécifiques développées plus avant. Elles sont constituées par *« les informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle »* des personnes. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes, mais les chercheurs bénéficient de certaines dérogations en cas de traitement de telles informations.

Constituent en effet des traitements de données personnelles : « la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » de données personnelles (art. 4 du RGPD).

POINTS CLÉS ET CONSEILS

- *Analyser préalablement la nature des données recueillies pour définir leur caractère personnel ou non. Repérer les recoupements et croisements possibles permettant l'identification des personnes concernées.*
- *Ne recueillir que les données strictement nécessaires.*
- *Identifier préalablement les données à caractère sensible.*

II - QUE DOIT-ON FAIRE LORSQU'ON TRAITE DES 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 ou diffusion ou toute autre forme de mise à disposition, rapprochement de données). Le support utilisé peut être matériel (fichier quel que soit son format, ou numérique).

Le principe retenu par le RGPD pour le traitement des données personnelles est celui de la responsabilisation ou « d'accountability ». Le système de responsabilisation recouvre à titre principal deux notions (art. 25 du RGPD) :

- **La protection des données dès la conception ou « Privacy by design »**
Le responsable de traitement anticipe, dès l'étape de définition d'un projet, toutes les contraintes juridiques en matière de protection des données personnelles ;
- **La protection des données par défaut ou « Privacy by default ».**
Le responsable de traitement doit s'assurer de ne collecter que les données strictement nécessaires aux finalités poursuivies par le traitement de données personnelles. On parle de principe de minimisation des données.

Une personne doit respecter les règles protégeant les données personnelles dès lors qu'elle effectue un « *traitement de données personnelles* » quel que soit son support.

Un chercheur ou une personne intervenant dans le cadre d'un travail requis à titre pédagogique est considéré comme traitant des données personnelles dès lors qu'il collecte des données individuelles au cours d'un entretien, mais aussi quand il prend en notes de telles données à partir d'un document qu'il consulte, ou qu'il envoie de telles données par mail à des tiers. Celui qui recueille l'information sera désigné sous le titre de « chercheur ».

POINTS CLÉS ET CONSEILS

- *Collecter des informations à titre individuel auprès d'une personne constituée en règle générale une donnée personnelle au sens du RGPD.*

- *Considérer la notion de traitement des données est conçue de façon très large par le RGPD intégrant la collecte, la consultation, la conservation, la communication, la destruction... de ces données.*
- *Intégrer la protection des données personnelles dès la conception du projet de recherche.*

III - LE RESPONSABLE DU TRAITEMENT DOIT ASSURER LA PROTECTION DES DONNÉES PERSONNELLES TRAITÉES.

Dès qu'un chercheur traite de telles informations, le responsable du traitement doit faire en sorte que les droits des personnes concernées soient respectés. Le responsable du traitement est selon le Règlement général sur la protection des données, « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Cette personne déterminant les finalités et les moyens d'un traitement de données personnelles, n'est pas nécessairement la personne physique qui concrètement consulte ou collecte les données personnelles (chercheur, ingénieur de recherche, élève ou étudiant...).

Le responsable du traitement des données est le directeur de l'EHESP. C'est le responsable du traitement qui prend toutes les mesures nécessaires à la préservation des droits des personnes concernées. Le chercheur intervient comme représentant du responsable du traitement des données. Le RGPD oblige tout organisme public à désigner un délégué à la protection des données (DPO, Philippe Marin pour l'EHESP) qui assiste le responsable du traitement de l'information et qui est par ailleurs le représentant de la CNIL dans l'institution.

POINTS CLÉS ET CONSEILS

- *Le directeur de l'EHESP est responsable du traitement des données personnelles au sein de l'Ecole. Il est à ce titre chargé d'assurer la protection des données personnelles traitées.*
- *Les chercheurs, étudiants, élèves recueillant des données personnelles agissent en tant que représentant du responsable du traitement de l'information.*
- *Le recueil de données personnelles par toute personne ayant un lien avec l'EHESP engage cette institution.*
- *Le DPO de l'EHESP est Philippe Marin, cil@ehesp.fr*

Pour se conformer aux règles fixées par le RGPD, le responsable du traitement des données personnelles ou son représentant doit procéder comme suit.

A) VÉRIFIER QUE LE TRAITEMENT DES DONNÉES PERSONNELLES EST LICITE (DONNER UNE BASE JURIDIQUE AU TRAITEMENT)

L'article 5.1-b) du RGPD prévoit que les données personnelles doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ses finalités...* ». Les données personnelles doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* » (art. 5.1-a) du RGPD).

Il résulte de ces dispositions que le responsable du traitement doit s'interroger sur la licéité du traitement dans le cadre de la recherche envisagée. En l'état, trois bases légales non cumulatives sont identifiées comme possible pour un traitement de recherche :

- 1- Le consentement des personnes.** Il constitue le premier fondement légal à envisager en application du principe général d'autodétermination informationnelle. Conformément à l'article 4.11° du RGPD, le consentement, est constitué par « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Un chercheur mène une enquête par entretiens ou questionnaires, et collecte à cette occasion des données personnelles. Le chercheur doit effectivement obtenir l'accord explicite des personnes concernées, pour mener cette collecte.
- 2- L'exécution d'une mission d'intérêt public.** Ce fondement implique l'existence d'un texte légal (en droit national ou en droit de l'Union Européenne) sur lequel le responsable du traitement peut se fonder pour mettre en œuvre son activité de recherche.
- 3- L'intérêt légitime du responsable de traitement.** Le recours à cette base légale implique de mettre en balance les intérêts du responsable du traitement avec ceux de la personne concernée et notamment de limiter les incidences négatives du traitement pour ces dernières. Dans l'hypothèse où les impacts négatifs sur les personnes seraient supérieurs aux intérêts poursuivis par le responsable du traitement, ce dernier doit mettre en œuvre des mesures compensatoires (par exemple le recours à l'anonymisation, ou à la sécurisation renforcée des données collectées). Un tel intérêt légitime peut, par exemple, exister lorsque la personne concernée est un client du responsable du traitement ou est à son service (Considérant 47 du RGPD). Ce motif peut servir de base juridique aux traitements par les services d'archives publiques (mission d'intérêt public). Il pourra difficilement constituer une base juridique pour les traitements effectués dans le cadre de la recherche (sauf en matière de recherche médicale et d'épidémiologie).

POINTS CLÉS ET CONSEILS

- *La première obligation repose sur l'obtention du consentement de la personne au recueil des données personnelles. Ce consentement doit être « libre, spécifique, éclairée et univoque ». Il est fortement conseillé de recueillir ce consentement par un document écrit.*
- *Les activités de recherche correspondent à des missions d'intérêt public constituent, l'un des fondements du recueil des données personnelles.*
- *L'intérêt légitime du responsable du traitement des données doit être mis en balance avec la préservation des intérêts de la personne interrogée. La personne assurant le recueil des informations doit notamment veiller à limiter les incidences négatives du traitement pour les personnes interrogées.*

B) RESPECTER SIX PRINCIPES GÉNÉRAUX LORS DU TRAITEMENT DES DONNÉES PERSONNELLES

Le responsable du traitement doit préalablement et jusqu'à la fin du traitement, respecter six principes généraux qui s'imposent notamment dans le cadre des programmes pédagogiques intégrant le recueil et le traitement de données personnelles.

- 1- **Licéité, loyauté et transparence du traitement.** Les données personnelles doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée* ». Cela signifie que les données ne doivent pas avoir été collectées, et ne doivent pas être traitées, sans que la personne concernée en ait connaissance. Ce principe nécessite de fournir aux personnes concernées plusieurs informations, sur la finalité du traitement, mais aussi sur les droits qu'ils peuvent exercer après la phase de collecte des données.
- 2- **La limitation des finalités.** Les données personnelles doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* ». Le RGPD prévoit toutefois que des données personnelles peuvent être traitées « *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* », même si elles n'avaient pas été initialement collectées à cette fin ; un tel traitement ultérieur n'est pas incompatible avec la finalité initiale de la collecte. C'est ce qui permet aux chercheurs de consulter des fonds existants contenant des données personnelles, sans enfreindre ce principe de limitation des finalités, et sous réserve de respecter certaines règles, comme par exemple les délais de consultation des archives publiques.
- 3- **La minimisation des données.** Seules doivent être collectées les données strictement nécessaires à la finalité du traitement.
- 4- **L'exactitude des données.** Les données personnelles collectées doivent être « *exactes et, si nécessaire, tenues à jour* » ; elles doivent sinon être rectifiées ou effacées.
- 5- **La limitation de la conservation.** Les données personnelles ne doivent pas être conservées au-delà de la durée nécessaire à la finalité du traitement. Le principe de limitation de la conservation implique que les personnes collectant soient en mesure de définir une durée de conservation proportionnée à la finalité poursuivie. Ce délai doit être présenté préalablement au recueil des informations et des données personnelles sollicitées.
Dans le cadre de travaux ponctuels, cette durée ne pourrait excéder la durée de présentation des travaux dans le cadre académique, à savoir une année au maximum. En outre, les représentants du responsable du traitement des données personnelles devront procéder à la suppression ou à l'archivage, le cas échéant dans les conditions prévues par le Code du patrimoine, des données en question à l'issue de la recherche, sauf justification particulière. A cet égard, le cycle de conservation des données peut être divisé en trois phases :

- la base active : elle correspond à la durée d'utilisation courante des données (en l'espèce, à la durée nécessaire à la réalisation des recherches) ;
- l'archivage intermédiaire : les données peuvent être conservées pour une durée plus longue en archivage intermédiaire, qui est distinct de la base active, et seulement pour un accès restreint (par exemple, s'il existe une obligation légale de conserver les données, si les données présentent un intérêt administratif ou, sous réserve de garanties appropriées, si les données sont traitées à des fins de recherche scientifique);
- l'archivage définitif : dans les conditions du Livre 2 du Code du patrimoine, l'intérêt public peut parfois justifier que certaines données ne fassent l'objet d'aucune destruction.

POINTS CLÉS ET CONSEILS

La conservation des données personnelles intègre successivement 3 bases :

- *la base active pour l'utilisation des données courantes ;*
- *la base intermédiaire qui permet un archivage intermédiaire et donne un accès restreint aux données ;*
- *l'archivage définitif permettant de préserver certaines données présentant un intérêt public au titre du patrimoine.*

- 6- **L'intégrité et la confidentialité des données.** Le responsable du traitement doit prendre « *les mesures techniques ou organisationnelles appropriées* » pour garantir la sécurité des données personnelles, y compris la protection contre le traitement non autorisé ou la perte des données. Cette obligation de prendre les mesures techniques ou organisationnelles appropriées est la pierre angulaire du RGPD.

Le responsable du traitement doit, pour garantir l'intégrité et la confidentialité des données personnelles traitées, vérifier que l'organisation (humaine) et les moyens techniques (souvent informatiques) mis en œuvre sont suffisamment sûrs pour protéger les droits et libertés des personnes concernées. Dans certains cas (les données sont sensibles, le traitement de données est mené à grande échelle...), le RGPD exige que soit également menée une étude d'impact approfondie Privacy Impact Assessment (PIA).

Enfin, dès lors que le chercheur a une base juridique pour traiter les données personnelles et qu'il respecte les six principes généraux indiqués ci-dessus, il doit enfin informer les personnes concernées et leur permettre d'exercer leurs droits, dans les conditions suivantes.

POINTS CLÉS ET CONSEILS

- *Six principes généraux doivent être respectés dans le traitement des données personnelles : 1) licéité, loyauté et transparence, 2) limitation des finalités, 3) minimisation des données, 4) exactitude des données, 5) limitation de la conservation des données, 6) intégrité et confidentialité des données ;*
- *Rédiger une notice d'information. Une information claire doit être délivrée à la personne auprès de laquelle on recueille des données personnelles. Cette information doit être écrite et doit rendre légitime le recueil de la donnée. ;*

- Le consentement de la personne enquêtée doit être recueilli formellement et par écrit. ;
- Les seuls supports techniques fiables permettant de collecter, traiter, transmettre, archiver... les données personnelles, sont ceux fournis par la direction des systèmes d'information et de des télécommunications (DSIT) de l'EHESP.

C) OBLIGATION D'INFORMER LES PERSONNES CONCERNÉES

Les deux premiers paragraphes de l'article 14 du RGPD établissent la liste des mentions d'informations que le responsable de traitement est tenu de délivrer aux personnes lorsqu'il traite des données qu'il n'a pas directement collectées auprès de celles-ci.

L'article 14.5-b) du RGPD prévoit que les informations fournies, par le responsable du traitement, à la personne concernée *« ne s'appliquent pas lorsque et dans la mesure où la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles »*.

Il résulte de ces dispositions que la collecte indirecte de données (s'agissant par exemple des données publiées figurant en ligne) peut être loyale même en l'absence d'information des personnes concernées. Pour cela le responsable du traitement doit-être en mesure de prouver l'impossibilité d'une telle collecte ou le caractère disproportionnés des efforts nécessaires pour informer les personnes, ou encore le fait que l'information des personnes compromettrait la réalisation des objectifs poursuivis par la recherche. Toutefois lorsque l'exception à l'information de la personne concernée prévue à l'article 14 du RGPD est invoquée par le responsable de traitement, l'étude ne peut entrer dans le cadre de la méthodologie de référence. Il doit donc saisir la CNIL d'une demande d'autorisation. **Information des patients mineurs ou des majeurs protégés.** Doivent également être destinataires de l'information :

- si la personne concernée est mineure : chacun des titulaires de l'autorité parentale ;
- si la personne concernée est un majeur protégé : le représentant légal ;
- si la personne concernée est hors d'état de recevoir l'information : les membres de la famille ou la personne de confiance. La personne concernée devra toutefois être informée si son état le permet par la suite.

Le RGPD prévoit une série de droits que les personnes peuvent faire valoir auprès des responsables de traitements qui traitent des données. S'agissant des traitements poursuivant des finalités de recherche, les droits suivants sont en principe applicables :

- 1) **droit à la transparence des informations, de communications** (art. 12 du RGPD) <https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence> ;
- 2) **droit à l'information** (art. 13 et 14 du RGPD) ;

- 3) **droit d'accès** (art. 15 du RGPD) <https://www.cnil.fr/fr/le-droit-dacces-connaître-les-donnees-quun-organisme-detient-sur-vous> ;
- 4) **droit de rectification** (art. 16 du RGPD) <https://www.cnil.fr/fr/le-droit-de-rectification-corriger-vos-informations> ;
- 5) **droit à l'effacement** (art. 17 du RGPD) <https://www.cnil.fr/fr/le-droit-leffacement-supprimer-vos-donnees-en-ligne> ;
- 6) **droit à la limitation du traitement** (art. 18 du RGPD) <https://www.cnil.fr/fr/le-droit-la-limitation-du-traitement-geler-lutilisation-de-vos-donnees> ;
- 7) **droit à la portabilité des données** (art. 20 du RGPD) : <https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions> ;
- 8) **droit d'opposition** (art. 21 du RGPD) : <https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees> .

POINTS CLÉS ET CONSEILS

La notice remise aux personnes dont les données personnelles sont collectées doit prévoir expressément les huit droits suivants qui doivent être précisés :

- droit à la transparence des informations et de la communication ;
- droit à l'information ;
- droit d'accès ;
- droit de rectification ;
- droit à l'effacement ;
- droit à la limitation du traitement ;
- droit à la portabilité des données ;
- droit d'opposition.

L'exercice de ces huit droits doit être garanti par la personne qui recueille les données personnelles pendant toute la durée de leur conservation.

L'exercice de ces droits doit être effectif et il se trouve placé sous la responsabilité de la personne qui recueille l'information. Il est conseillé dans tous les cas de fournir les coordonnées du DPO de l'EHESP cil@ehesp.fr

IV - LES DONNÉES SENSIBLES (OU « CATÉGORIES PARTICULIÈRES DE DONNÉES »)

Les données sensibles forment une catégorie particulière des données personnelles. Ce 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 RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas :

- 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 rendues publiques par la personne concernée ;
- Si elles sont nécessaires à la sauvegarde de la vie humaine en particulier si elles sont nécessaires dans un but médical ou pour la recherche dans le domaine de la santé ;
- 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 ou syndicale.

Les données personnelles concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Les données de santé sont des données personnelles particulières, faisant l'objet d'une protection renforcée dans les textes (RGPD, Loi Informatique et Libertés, Code de la santé publique, etc....) afin de garantir le respect de la vie privée des personnes.

Dans tous les cas, il est conseillé de contacter le DPO de l'EHESP (cil@ehesp.fr) pour être guidé dans les démarches à réaliser.

La CNIL a adopté des nouvelles Méthodologies de référence (MR). Les recherches menées au sein de l'EHESP sont principalement concernées par les méthodologies MR-001, MR-003 et MR-004, qui offrent un cadre sécurisé pour la mise en œuvre des traitements de recherche dans le domaine de la santé. Ces référentiels encadrent les traitements de données de santé à des fins de recherche. Si le traitement est conforme à l'une de ces méthodologies, la demande d'autorisation n'est pas nécessaire. L'EHESP est enregistrée auprès de la CNIL pour être autorisée à utiliser les 6 MR publiées par la CNIL.

Le recours aux différentes MR doit faire l'objet d'une inscription au répertoire public des études réalisées sous MR ; cette inscription est faite par le DPO sur le site internet du Système national des données de santé (SNDS).

Toute difficulté d'interprétation ou d'application du présent guide doit faire l'objet d'une saisine auprès du DPO de l'EHESP : cil@ehesp.fr.

Document validé par le Comité Informatique et Libertés le 25 novembre 2019

Document validé par le Comité de Direction (CODIR) le 20 janvier 2020

Fait à Rennes, le 20 janvier 2020

Annexes

MR001 : Recherches dans le domaine de la santé avec recueil du consentement.

MR002 : Études non interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro

MR003 : Recherches dans le domaine de la santé sans recueil du consentement.

MR004 : Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé.

MR005 : Études nécessitant l'accès aux données du PMSI et/ou des RPU par les établissements de santé et les fédérations hospitalières

MR006 : Études nécessitant l'accès aux données du PMSI par les industriels de santé