Les projets de recherche « internationaux » et la protection des données

Fiche pratique

****

Contexte et cadre général

De nombreux projets de recherche, au sein de laboratoires dont le CNRS est tutelle, comportent une dimension internationale, parce que les terrains d'étude se situent à l'étranger et/ou par le biais de collaborations de recherche internationales*.

Dans le cadre de ces projets, plusieurs règlementations relatives à la protection des données peuvent s'appliquer : la règlementation française et européenne (Règlement Général sur la Protection des Données - RGPD, la Loi Informatique et Libertés, modifiée - LIL) et les règlementations en vigueur localement selon les pays et régions du monde concernés par les projets de recherche (si elles existent, la loi relative à la protection des données du pays concerné, d'autres lois sectorielles ainsi que les règles communautaires).

Cette fiche pratique a pour but d'aider la communauté scientifique CNRS, impliquée dans des projets de recherche à dimension internationale, à comprendre et à appliquer les règles lorsque des données à caractère personnel de résidents hors de l'UE sont traitées dans ces projets. Elle présente les démarches à suivre et les services à contacter pour un accompagnement adapté à chaque projet.

*** NB** : Cette fiche ne s'applique pas :

- Aux simples transferts de données vers des partenaires ou prestataires installés dans des pays étrangers à l'UE ; dans ces cas, veuillez contacter le service protection des données en charge de votre unité. Pour le CNRS : SPD – dpd.demandes@dpd-cnrs.fr

- Aux traitements de données de résidents de l'espace économique européen (UE + Islande + Liechtenstein + Norvège) dans le cadre de projets de recherches accueillant des chercheurs internationaux au sein des Unités en France ; dans ces cas, veuillez contacter le service protection des données de votre unité ainsi que le fonctionnaire sécurité et défense compétent. Pour le CNRS : FSD : cnrs.fsd@cnrs.fr .

Quelques définitions

Donnée à caractère personnel : toute information se rapportant à une personne physique vivante (ou décédée, dans certains cas) identifiée ou identifiable directement ou indirectement. *Ex : nom et prénom, numéro de téléphone, commune d'habitation…*

Personne concernée : une personne physique identifiée ou identifiable dont les données à caractère personnel sont traitées. *Ex : participants à la recherche, dans le cadre de projets de recherche*

Traitement de données : toute opération portant sur des données à caractère personnel ou tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés (format numérique ou papier). *Ex : consultation d'un fichier, enregistrement audiovisuel, analyse, stockage ou hébergement…*

Réutilisation de données : toute opération portant sur des données à caractère personnel, produites par une entité, à des fins autres que celles initiales. *Ex : réutilisation d'informations issues d'un précédent projet de*

recherche pour atteindre les objectifs d'un nouveau projet, consultation ou obtention d'une base de données produite par une administration à des fins de recherche.

Responsable de traitement : 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. En pratique, au CNRS, les directeurs ou directrices d'unités sont responsables de traitement des données mis en œuvre au sein de leurs unités.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données pour le compte du responsable de traitement. *Ex : une entreprise suisse qui héberge des données d'un projet de recherche porté par un laboratoire CNRS.*

Six bonnes pratiques

1. Réaliser les démarches selon le(s) pays concerné(s)

Les démarches de protection des données varient d'un pays à un autre, d'une législation à une autre.

Si en France, depuis 2018[1], l'autorité de protection des données (CNIL[2]) est sollicitée uniquement dans des cas complexes de traitement de données, dans certains pays, l'intervention de l'autorité est beaucoup plus régulière. Par exemple, la loi ivoirienne exige d'obtenir une autorisation de l'autorité de protection des données avant tout traitement de données personnelles pour motif public à des fins scientifiques ainsi qu'avant tout transfert de données en dehors du territoire ivoirien.

Il est donc important que soient identifiées en amont du projet de recherche les lois qui peuvent s'y appliquer afin de déterminer les démarches à accomplir.

Si le pays concerné ne dispose pas de loi en matière de protection des données, les démarches seront réalisées conformément à la règlementation européenne.

Qui contacter ?

Le **délégué à la protection des données compétent** (pour le CNRS : dpd.demandes@dpd-cnrs.fr) pour identifier les lois applicables et accompagner dans les démarches de conformité relatives au projet.

2. Déterminer les rôles et responsabilités pour chaque projet de recherche

Dans le cadre de projets de recherche « internationaux », différents acteurs peuvent être impliqués. Plusieurs cas de figure sont alors envisageables.

- Le projet implique uniquement le laboratoire dont le CNRS est tutelle et l'équipe de recherche du laboratoire définit seule les orientations scientifiques du projet. Dans ce cas, le responsable de traitement est le directeur ou la directrice de l'Unité ;
- Le projet implique plusieurs acteurs/organismes (universités, établissements de recherche, laboratoires, entreprises…) autres que le laboratoire dont le CNRS est tutelle. Dans ce cas, une qualification des rôles doit être faite.

[1] Année d'entrée en application du Règlement général sur la protection des données (RGPD)

[2] Commission Nationale Informatique et Libertés

- Si les acteurs définissent conjointement les moyens et les objectifs de traitement de données pour le projet, ils seront considérés comme **responsables conjoints ou co-responsables de traitement**. *Ex : des chercheurs d'une UMR CNRS et des chercheurs d'un laboratoire philippin déterminent ensemble les méthodes et orientations scientifiques d'une enquête dans le cadre d'un projet. Les deux entités sont co-responsables ou sont responsables conjoints du traitement.*

- Si les acteurs définissent chacun les moyens et finalités des traitements de données qu'ils réalisent dans le cadre du projet, ils seront considérés comme **responsables disjoints ou distincts de traitement**. *Ex : Dans le cadre d'une enquête réalisée auprès d'étudiants au Canada, une Unité CNRS et une Université canadienne collaborent. L'Unité analyse les données de l'enquête pour comprendre l'évolution de l'apprentissage la langue française dans les provinces anglophones. De son côté, l'Université utilise ces données pour mettre à jour ses plaquettes de formation en faculté de lettres. Les deux structures seront considérées comme responsables disjoints ou distincts du traitement.*
  C'est aussi la même qualification en cas de réutilisation de données. Le producteur initial de la base de données personnelles et le ré-utilisateur de cette base sont qualifiés de responsables disjoints ou distincts.

- Si l'autre ou les autres acteurs impliqués l'est / le sont en tant que prestataire (s) du laboratoire CNRS, on parlera de **sous-traitance au sens de la protection des données**. *Ex* : *Des chercheurs d'une UMR CNRS réalisent une enquête terrain à Madagascar. Afin de faire passer les questionnaires aux participants à la recherche, une entreprise locale a été recrutée. Cette dernière est qualifiée de « sous-traitant » au sens de la protection des données.*

Ces différentes qualifications ainsi que les relations avec les autres acteurs doivent être définies dans un document contractuel.

Pour information : *Les acteurs n'ont pas besoin d'accéder aux données ou de les manipuler pour être qualifiés de responsables de traitement.*

Ex : Une Unité CNRS en France collabore avec une équipe de recherche au Liban. Les chercheurs de l'Unité CNRS participent à définir les finalités et méthodes scientifiques à employer dans le cadre du projet ainsi que les outils de collecte de données. Ils ne se déplacent pas sur le terrain d'enquête au Liban, ils n'accèdent aucunement aux données identifiantes collectées, ils sont simples destinataires des données agrégées par le partenaire Libanais. Pour autant, l'Unité CNRS sera responsable de traitement conjoint parce qu'elle a participé à la définition des objectifs et moyens du traitement de données dans le cadre du projet.

Qui contacter ?

- Le **délégué à la protection des données compétent** pour conseiller dans la qualification des rôles et responsabilités du traitement de données dans le cadre du projet.

- Le **gestionnaire de contrat compétent** pour le laboratoire concerné ou, selon les cas, la **direction Europe et international (DEI)** du CNRS pour la détermination de la nature du contrat (contrat de collaboration de recherche, contrat de prestation de service…), sa signature et son suivi.

3. Définir un (des) fondement (s) légal (aux) *justifiant le traitement des données*

Tout traitement de données à caractère personnel doit avoir un fondement légal. C'est ce qui justifie l'utilisation des données.

Dans la règlementation en vigueur en France et en Europe, il existe six différentes bases légales pouvant fonder le traitement des données[3]. Contrairement à cette règlementation qui laisse le choix de la base légale au responsable de traitement (à condition de pouvoir justifier son choix), certains pays imposent une base légale unique pour tout traitement de données.

Le CNRS et ses laboratoires, étant territorialement rattachés à la France, utilisent les bases légales applicables en France (et en Europe). Celle la plus utilisée dans le cadre des projets de recherche au CNRS est la mission d'intérêt public puisque lesdites recherches entrent dans la mission de service public du CNRS, définie dans le Code de la recherche[4].

Lorsque le traitement de données implique l'international, ce fondement juridique peut être insuffisant. Il convient alors de fonder le traitement, au-delà de notre mission d'intérêt public, sur une base légale établie par la législation du pays et ou de la région du monde concernée.

A titre d'illustration, dans le cadre d'un projet de recherche d'un laboratoire CNRS avec pour terrain d'enquête l'Equateur, les fondements légaux du traitement de données seront, d'une part, la mission d'intérêt public (règlementation européenne et française, par le rattachement territorial de la structure) et, d'autre part, le consentement des participants à la recherche (législation équatorienne, du fait du lieu de résidence des participants à la recherche).

Pour information : *Le fondement légal le plus présent dans différentes législations du monde est le consentement.*

Qui contacter ?

- Le **délégué à la protection des données compétent** pour accompagner dans la détermination des bases légales conformes au projet et aux lois applicables.

4. Informer les personnes concernées *par le traitement des données*

Informer les personnes dont les données sont traitées est une obligation quels que soient les textes applicables dans ou hors de l'Union européenne.
Ainsi, pour tout projet de recherche à dimension internationale, les participants à la recherche devront être informés, à minima : des objectifs du projet, des coordonnées du/des responsable(s) de traitement et du/des délégué(s) à la protection des données, du/des fondement(s) légal(aux) retenu(s), des destinataires des données, de la durée de conservation des données, de leurs droits, du transfert de leurs données hors de leur pays de résidence.

Cette information peut prendre diverses formes. Elle peut être directe (c'est-à-dire fournie aux personnes directement) dans le cadre de projets nécessitant une collecte des données auprès des personnes concernées ; elle peut également être indirecte dans le cas des réutilisations de données, si la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. Dans ce dernier cas, l'information peut être rendue publique, par exemple, via le site internet de l'Unité concernée.

Dans tous les cas, l'information apportée aux personnes doit être faite de sorte à être comprise de ces dernières. Il faudrait que les personnes s'engagent volontairement dans le projet en ayant bien assimilé tous les enjeux. Ainsi, par exemple :

- *Pour un projet de recherche se déroulant auprès d'hindiphones, notre obligation d'information des personnes ne serait pas respectée si nous fournissons une information en langue française ; dans ce cas, il faudrait envisager de passer par un traducteur ;*

[3] Article 6 du RGPD : le consentement de la personne concernée, le contrat auquel la personne concernée est partie, l'obligation légale du responsable de traitement, la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, intérêts légitimes poursuivis par le responsable du traitement ou par un tiers…
[4] Chapitre II, Titre II du Livre III de la partie règlementaire du code de la recherche

- *Pour une recherche auprès de populations analphabètes, la fourniture d'un document papier à titre d'information ne serait pas adaptée ; dans ce cas, une information orale pourra être privilégiée.*

Pour information : *Il existe certains modèles de notices d'information des participants à la recherche rédigés par le SPD du CNRS et conformes aux législations de certains pays.*

Qui contacter ?

Le **service protection des données (SPD)** du CNRS pour accéder à un modèle (s'il existe pour le pays de votre étude) ou pour accompagner dans la rédaction de la notice d'information adaptée à votre projet et tenant compte du pays ou de la région du monde concernée.

*5. **Assurer la sécurité des données** tout au long du projet*

La sécurisation des données est un des grands principes de la protection des données. Lorsque les projets de recherche sont réalisés dans un contexte international, les risques pour la sécurité des données sont plus accrus.

Afin d'éviter la perte des données, l'accès ou la modification de ces dernières par des personnes non autorisées, il est important de respecter les règles relatives à la sécurité des données issues de la règlementation ainsi que celles des tutelles. Par exemple, le Fonctionnaire sécurité et défense (FSD) et le Responsable national de la sécurisation des SI (RSSI-N) du CNRS, ont formulé des recommandations sur les conditions d'emport et d'utilisation des ordinateurs portables et autres outils informatiques à l'étranger[5].

Concrètement :

- Au moment de la collecte, les données doivent être recueillies à l'aide d'outils professionnels sécurisés (ordinateurs, dictaphones, liens et espaces sécurisés ...). Par exemple, les ordinateurs doivent être chiffrés conformément aux recommandations du FSD[6] et à la note du DGDR[7]. Les sous-traitants éventuellement recrutés pour la collecte devront présenter des garanties de sécurité de leurs outils et respecter les engagements qui seront pris dans le contrat conclu avec eux.

- Pendant la durée du projet, les données doivent être traitées avec des outils sécurisés et stockées sur des serveurs sécurisés. La direction interministérielle du numérique, le CNRS ainsi que les tutelles partenaires proposent des outils sécurisés accessibles à toute la communauté CNRS[8]. Dans les collaborations avec des partenaires sur le terrain d'enquête, les outils proposés par ces derniers pour traiter les données doivent également être conformes au cadre règlementaire.

- A la fin du projet, les données pourront être supprimées, anonymisées ou archivées conformément à la règlementation en vigueur. En cas de partage des données dans le cadre de la science ouverte, celles-ci devront être anonymisées, pseudonymisées ou faire l'objet de conventions spécifiques garantissant sécurité et confidentialité des données.

Toutefois, certaines mesures de sécurité ne peuvent être applicables sur certains terrains d'étude étrangers.

Pour information : *Dans certains pays, par exemple, il est interdit d'avoir des outils chiffrés. Dans de tels cas, des recommandations spécifiques sont faites pour garantir la sécurité des données (octroi d'un ordinateur vierge, dépôt des données directement sur des espaces sécurisés du CNRS depuis le pays concerné etc..).*

[5] Note du FSD du 29 avril 2009, https://intranet.cnrs.fr/protection_donnees/seformer-sensibiliser/Documents/consignes-portables-etranger.pdf
[6] Recommandations du 17 avril 2008, https://intranet.cnrs.fr/protection_donnees/seformer-sensibiliser/Documents/Recommandation-protection-donnees-chiff.pdf
[7] Note du 30 novembre 2018, https://intranet.cnrs.fr/protection_donnees/seformer-sensibiliser/Documents/20181130%20Note%20chiffrement%20ordi.pdf
[8] Outils et services informatiques, https://intranet.cnrs.fr/Cnrs_pratique/si/Pages/default.aspx

Dans tous les cas, une analyse d'impact relative à la protection des données[9] devra être réalisée si le projet présente une sensibilité particulière ou si le pays concerné par le terrain d'étude exige cette analyse avant tout traitement de données hors de son territoire par une structure étrangère.

Qui contacter ?

Le **Fonctionnaire sécurité et défense (FSD)** du CNRS pour des recommandations précises selon les pays du monde concernés par le projet de recherche.

Le **service protection des données (SPD)** du CNRS pour accompagner dans la conformité avec les exigences de sécurité du pays concerné.

La personne **chargée de la sécurité des systèmes d'information (CSSI)** de l'Unité ou la personne **responsable de la sécurité des systèmes d'information (RSSI)** de la délégation régionale de rattachement pour mettre en place les mesures concrètes de sécurité sur vos outils.

6. Garantir les droits des personnes

Toute personne qui participe à un projet de recherche pour lequel ses données personnelles sont traitées dispose de droits qui lui sont reconnus par les textes en vigueur en matière de protection des données.

Les participants à des projets internationaux ont ainsi droit d'accéder et d'obtenir copie des données les concernant, de s'opposer au traitement de ces données ou de les faire rectifier, de demander la limitation du traitement de leurs données, leur portabilité et leur suppression ; le cas échéant, de demander à retirer leur consentement et de faire une réclamation auprès de l'autorité de protection des données.

Pour information : *Les droits accordés aux personnes peuvent varier en fonction de leur pays et de la/des base(s) légale(s) applicable(s).*

Les personnes doivent être informés des moyens mis à leur disposition pour exercer ces droits. Dans le cadre des projets internationaux, il faudra favoriser les demandes d'exercice de droits en rendant accessibles les moyens mis à disposition. *A titre d'illustration, dans un projet avec pour terrain l'Australie, il serait plus judicieux de laisser des coordonnées d'adresse électronique aux personnes souhaitant exercer leurs droits plutôt que l'adresse postale de l'Unité en France, ce qui exigerait des coûts à la personne concernée.*

Qui contacter ?

Le **service protection des données (SPD -** dpd.demandes@dpd-cnrs.fr**)** du CNRS pour apporter les conseils, instruire les demandes et conserver la documentation relative aux demandes dans le registre d'exercice des droits dédié.

[9] L'analyse d'impact (AIPD) permet d'évaluer, au regard des mesures de sécurité mises en place dans le cadre d'un projet, la persistance ou non de risques sur la vie privée des personnes concernées.