CONFORMITÉ RGPD ET RECHERCHE EN SHS

Mode d'emploi pour les chercheurs de Paris 1 Panthéon-Sorbonne

Dernière modification : 24-03-2025

INTRODUCTION

Qu’est-ce que le RGPD ?

Les sciences humaines et sociales (SHS) sont particulièrement impliquées dans le traitement de données issues d'enquêtes, d'entretiens ou de thématiques sensibles. Dans ce contexte, le respect des normes éthiques et légales est essentiel. Depuis 2018, une réglementation européenne a été mise en place, renforçant les obligations des laboratoires et du personnel de recherche concernant la gestion des données, et plus spécifiquement des données personnelles.

Le Règlement Général sur la Protection des Données (RGPD), adopté en mai 2018, est une loi européenne visant à protéger les informations personnelles des citoyens de l'Union européenne. Il a pour objectif de renforcer le contrôle des individus sur leurs données personnelles tout en établissant un cadre de gestion pour ceux qui les manipulent, en imposant diverses obligations légales. Il encadre le traitement des données à caractère personnel, définissant des actions telles que la collecte, l’enregistrement, la conservation, l’utilisation, la communication, ou encore l’effacement des données, et ce, dans un contexte où des géants technologiques comme les GAFA utilisent massivement nos données personnelles. Dans ce cadre, **le RGPD interroge la communauté scientifique, notamment dans les domaines des sciences humaines et sociales, quant à la compatibilité des travaux de recherche avec la réglementation**.

Suis-je concerné(e) par le RGPD dans le cadre de la recherche ?

Le respect du RGPD est une obligation légale européenne qui s’applique également au domaine de la recherche scientifique (selon le considérant 159), dans son sens large, incluant la recherche publique, privée et appliquée. Le Comité européen de la protection des données (CEPD), dans ses lignes directrices sur le consentement, apporte un éclairage supplémentaire en indiquant que la recherche scientifique se caractérise par « *un projet de recherche établi conformément aux normes méthodologiques et éthiques du secteur en question, conformément aux bonnes pratiques* ».

En ce sens, l’Organisation de Coopération et de Développement Économique (OCDE) définit les données de la recherche comme « *des enregistrements factuels (chiffres, textes, images et sons), utilisés comme sources principales pour la recherche scientifique et généralement reconnues par la communauté scientifique comme nécessaires pour valider les résultats de la recherche* ».
Ces données peuvent prendre diverses formes, telles que des données d’observation, d’expérimentation, de simulation, ou de référence. Toutefois, certaines de ces données peuvent être à caractère personnel, c’est-à-dire contenir des informations permettant d'identifier, directement ou indirectement, une personne physique, comme un email, un numéro de téléphone, ou même des préférences personnelles.
Compte tenu de cette définition large, la notion de « recherche scientifique » peut s’appliquer aux traitements, collectes et utilisations de données personnelles menées dans le cadre de thèses de doctorat ou de mémoires de recherche, par des chercheurs rattachés à une université ou à un autre établissement d’enseignement supérieur, des laboratoires de R&D, etc. Ainsi, les SHS sont particulièrement exposées au traitement de données personnelles car elles impliquent souvent l’étude de populations, de comportements, d’opinions ou de parcours individuels, à travers des enquêtes, des entretiens ou l’analyse de sources contenant des informations identifiantes.

Même si les résultats finaux sont présentés sous forme de données anonymisées ou agrégées, il est crucial de garder à l'esprit que, avant cette étape de publication, les données personnelles sont bien souvent manipulées. Par conséquent, la plupart des chercheurs collectent et traitent des données personnelles, parfois sans en être pleinement conscients. Cela **vous rend responsables de la conformité avec le RGPD**, afin de garantir la protection et la confidentialité de ces informations à toutes les étapes du processus de recherche.

Les situations où vous pouvez réellement affirmer que le RGPD ne s'applique pas sont en réalité assez rares :
- Lorsque le traitement ne concerne aucune donnée personnelle. Par exemple, une étude sur le métabolisme des oiseaux migrateurs ou des recherches sur les satellites de Jupiter.
- Lorsque les données traitées sont totalement anonymisées, c'est-à-dire qu'elles ne permettent plus d'identifier une personne de manière directe ou indirecte (ce qui est complexe à réaliser en pratique).
- Lorsque le responsable du traitement n'est pas établi dans l'UE et que les recherches ne concernent aucune personne située sur le territoire de l'Union.

Quelle importance le RGPD a-t-il dans mes travaux de recherche ?

La mise en conformité au RGPD nécessite un investissement conséquent, mais ne doit pas être perçu comme un obstacle à vos recherches, mais plutôt comme un **atout stratégique**. En prenant en compte les exigences liées à la protection des données personnelles, vous pouvez gérer vos données de recherche de manière plus responsable, éthique et conforme. À long terme, cette démarche **présente de nombreux bénéfices** : amélioration de la qualité de vos travaux, facilitation de la réutilisation et du partage des données (démarche de science ouverte), prévention des risques juridiques, renforcement de votre réputation et de crédibilité, confiance des participants… De plus, les organismes de financement sont de plus en plus attentifs à ces enjeux, et **le respect de la réglementation européenne constitue souvent un véritable atout pour distinguer les candidatures**. Enfin, il n'est pas rare que certains organismes vous demandent des preuves de votre conformité RGPD lors de l'établissement de convention de recherche (exemple de la DARES notamment) ou lors d'une demande de publication auprès d'éditeurs.

À titre d'exemple, si une violation du RGPD est constatée par des tiers, les conséquences peuvent être lourdes. En plus de la perte des avantages mentionnés précédemment, l'établissement s'expose à :
- L'engagement de sa responsabilité civile en cas de préjudice causé par la violation des données personnelles.
- D'éventuelles sanctions pénales pouvant aller jusqu'à 300 000 € d'amende et 5 ans d'emprisonnement.
- Une sanction administrative, notamment en cas d'action de la CNIL ou d'une autre autorité de contrôle.

En outre, le véritable risque ne réside pas uniquement dans la sanction légale, mais surtout dans l'impact sur l'image de l'université. En tant qu'établissement public, nous nous devons de traiter les données avec intégrité et rigueur scientifique. Si des pratiques illégales sont découvertes, cela engendre une perte de confiance qui, malheureusement, affecte l'ensemble de la communauté universitaire.

Comment me mettre en conformité avec le RGPD pour m'acquitter de mes obligations ?

Le principe de "**responsabilité**", pilier essentiel du RGPD, signifie que **vous devez être en mesure de démontrer, à tout moment, que vous prenez les mesures nécessaires pour protéger les données personnelles** utilisées dans le cadre de vos recherches.

Toutes les preuves de cette démarche doivent être consignées de manière claire et détaillée dans un document intitulé "**fiche de traitement des données**", qui sera associée à votre projet de recherche. Ce document, lorsqu'il est correctement rempli, recense l'ensemble des démarches et informations essentielles pour garantir la conformité au RGPD. **En maintenant cette fiche à jour, vous disposerez d'une preuve tangible de votre conformité**.
Une fois complétées par les chercheurs, ces fiches sont ensuite conservées par le **Délégué à la Protection des Données** (DPO) de votre établissement dans un espace appelé "**registre des traitements de données**". Ce registre centralise et décrit tous les traitements de données personnelles effectués au sein de l'établissement, le DPO jouant ici un rôle comparable à celui d'un notaire, responsable de la conservation de ces documents juridiques.

La conservation de la fiche de conformité par le DPO n'est donc pas anodine : elle garantit la continuité dans la gestion des informations personnelles au fil du temps. Le DPO consacre ainsi une part importante de son temps à identifier les personnes manipulant des données personnelles, à les informer de leurs responsabilités, et à les accompagner dans la complétion de leur fiche dans le registre des traitements.
L'université Paris 1 Panthéon-Sorbonne compte 37 laboratoires de recherche en SHS, dont 13 unités propres et 24 unités mixtes de recherche en cotutelle avec d'autres organismes de recherche. En raison de ce nombre, il est malheureusement **impossible pour le DPO de suivre individuellement chaque étudiant, doctorant ou chercheur manipulant des données personnelles** pour leur expliquer ou leur rappeler de devoir prendre le temps de remplir une fiche dans le registre des traitements. **Il vous revient donc de prendre directement contact avec le DPO pour vous signaler et demander la création de cette fiche** (cf. partie suivante sur comment identifier son DPO).

À noter : le DPO a pour mission d'informer, de conseiller et d'éclairer sur l'application du RGPD. Il n'est ni responsable des manquements ou violations, ni chargé de remplir les fiches du registre à votre place. Ces obligations incombent exclusivement au responsable du traitement, qui en assume l'entière responsabilité.

Une fois la fiche créée, vous pourrez la compléter en toute autonomie. Elle devra être **mise à jour régulièrement** en fonction de l'évolution de votre méthodologie de recherche ou de tout changement dans la gestion des données personnelles (par exemple, en cas de réalisation d'enquêtes, de collecte de données supplémentaires, ou de nouveaux partages de données prévus). N'hésitez donc pas à la faire évoluer en parallèle de vos recherches.
Enfin, gardez à l'esprit que, bien qu'il s'agisse d'un document interne à l'établissement, **cette fiche doit pouvoir être communiquée et consultée par la Commission nationale de l'informatique et des libertés** (CNIL), l'organisme de régulation et de contrôle des données personnelles en France. En cas de demande ou d'audit de leur part, vous devrez être en mesure de présenter cette fiche ainsi que les efforts entrepris pour garantir la conformité de votre projet (cf. sanctions possibles en cas de violation du RGPD).

Comment remplir une fiche dans le registre de traitement ?

Il s'agit d'un **formulaire en ligne comportant de nombreux champs**, dans lequel vous devez répondre de manière détaillée et argumentée à plusieurs questions couvrant divers aspects du RGPD. Pour vous donner une idée, voici certains des éléments abordés : la raison et la légalité de la collecte des données, les personnes concernées, les types de données collectées, les destinataires des données, les modalités d'hébergement et de stockage, la durée de conservation prévue…

Compléter la fiche de traitement n'est pas particulièrement complexe, mais **nécessite du temps**, de la réflexion et un recul sur la méthodologie de recherche la plus appropriée. L'objectif n'est pas de ralentir ou de compliquer votre travail de recherche, mais plutôt d'intégrer cette démarche de conformité en parallèle de vos activités. Plus tôt vous commencerez, mieux ce sera, même si certaines questions n'auront peut-être pas de réponses immédiates. Cela vous permettra néanmoins de mieux orienter vos réflexions futures, car une fois un projet de recherche sur le point de se clôturer, il devient extrêmement difficile, d'intervenir pour corriger certains écarts avec la réglementation. C'est pourquoi il est essentiel de mener ces réflexions **AVANT** de commencer la collecte, le traitement et l'analyse des données.

Ainsi, dès que possible, **prenez contact avec le DPO de votre établissement pour demander la création de votre fiche dans le registre des traitements**. Cette fiche sera directement liée à votre projet, et vous pourrez la gérer en toute autonomie grâce à un **accès unique via un lien internet** que nous vous fournirons.
Une fois le lien vers votre fiche de registre fourni, vous pouvez commencer à la remplir en cliquant sur « **Modifier** » (« **Edit** » en version anglaise) dans la barre d'actions située en haut de la page. Je vous recommande de **sauvegarder régulièrement vos modifications** en cliquant sur « **Enregistrer** » au bas de la page. Cela vous permettra de suivre l'avancement de votre travail sans risquer de perdre vos informations.

Comment identifier et contacter mon DPO ?

Pour commencer la mise en conformité de vos travaux, vous devrez prendre contact avec votre DPO. Il est important **d'identifier précisément le DPO de votre établissement**, car plusieurs structures peuvent être impliquées dans la gestion des données (notamment pour les organismes concernés par une cotutelle).

En principe, chaque organisme traitant régulièrement des données personnelles (comme les universités, les grandes écoles ou les laboratoires de recherche) a l'obligation de **déclarer officiellement son DPO auprès de la CNIL**. Cette déclaration formalise le choix du DPO, qui doit accepter la mission proposée et s'engage donc, en tant que conseiller, à intervenir sur un périmètre bien défini. Malheureusement, certaines structures n'ont parfois pas encore effectué cette déclaration, ce qui peut rendre l'identification du DPO responsable plus complexe.

Votre première action sera donc de **vérifier quel est le DPO en charge du périmètre de l'organisme de recherche auquel vous êtes rattaché(e)**, car selon votre structure, votre interlocuteur en matière de conformité pourrait être le DPO de l'Université Paris 1 Panthéon-Sorbonne, ou celui d'une autre entité, comme le CNRS (dpd.demandes@cnrs.fr) ou l'Université Paris 8 (dpo@univ-paris8.fr) :

- Si vous êtes affilié(e) à une UFR ou une Unité de Recherche (UR), le DPO à contacter est celui de l'Université Paris 1 Panthéon-Sorbonne à l'adresse suivante dpo@univ-paris1.fr et la méthodologie à appliquer et celle présentée dans ce guide pratique.

- Pour les Unités Mixtes de Recherche (UMR), la situation est plus complexe, car chaque établissement a le choix de son propre DPO. Il est donc essentiel d'identifier précisément le DPO désigné auprès de la CNIL pour votre UMR. Pour vous aider, nous avons établi un tableau de correspondance présenté ci-dessous.
Si le DPO n'a pas encore été désigné pour votre UMR, cela signifie probablement que la déclaration CNIL n'a pas encore été finalisée. Dans ce cas, contactez votre Directeur d'Unité (DU) pour obtenir des informations sur l'avancement des démarches.

Intitulé de l'unité mixte de recherche	Acronyme	Sigle de l'unité	DPO désigné
Anthropologie et Histoire des Mondes Antiques	ANHIMA	UMR 8210	CNRS
Archéologie des Amériques	ARCHAM	UMR 8096	CNRS
Archéologies et Sciences de l'Antiquité	ARSCAN	UMR 7041	Pas de désignation
Centre d'Économie de la Sorbonne	CES	UMR 8174	CNRS
Centre européen de sociologie et de science politique	CESSP	UMR 8209	CNRS
Centre d'histoire sociale des mondes contemporains	CHS	UMR 8058	CNRS
Développement et Société	DEVSOC	UMR 201	Non identifié
Géographie-Cités	GC	UMR 8504	CNRS
Antiquité, moyen-âge, transmission Arabe [équipe interne de SPHERE - Sciences, Philosophie, Histoire - UMR 7219]	GRAMATA (SPHERE)	UMR 7219	CNRS
Institutions et Dynamiques Historiques de l'Economie et de la Société	IDHES	UMR 8533	Paris 8
Institut d'histoire moderne et contemporaine	IHMC	UMR 8066	CNRS
Institut d'histoire et de philosophie des sciences et des techniques	IHPST	UMR 8590	Non identifié
Institut des mondes africains	IMAF	UMR 8171	CNRS
Institut des Sciences Juridique et Philosophique de la Sorbonne	ISJPS	UMR 8103	CNRS
Laboratoire dynamiques sociales et recomposition des espaces	LADYSS	UMR 7533	CNRS
Laboratoire de Médiévistique Occidentale de Paris	LAMOP	UMR 8589	CNRS
Laboratoire de Géographie Physique : Environnements Quaternaires et Actuels	LGP	UMR 8591	CNRS
Mondes américains	Mondes Américains	UMR 8168	CNRS
Orient et Méditerranée, textes - archéologie - histoire	OMTAH	UMR 8167	CNRS
Paris Jourdan Sciences Économiques	PjSE	UMR 8545	CNRS
Pôle de recherche pour l'organisation et la diffusion de l'information géographique	PRODIG	UMR 8586	CNRS
Sorbonne-Identités, relations internationales et civilisations de l'Europe	SIRICE	UMR 8138	Non identifié
Technologie et Ethnologie des Mondes PréhistoriqueS	TEMPS	UMR 8068	CNRS
Trajectoires de la sédentarisation à l'état	Trajectoires	UMR 8215	CNRS

Comment utiliser le kit de conformité efficacement ?

Nous sommes conscients que le RGPD peut sembler complexe, et que certains d'entre vous n'y ont peut-être jamais été confrontés. Il est donc normal de se demander comment être sûr que vos réponses et réflexions respectent pleinement la législation. Pas de panique, c'est précisément pour cela que nous avons créé ce kit de conformité. Ce guide regroupe tous les conseils, bonnes pratiques et points de vigilance nécessaires. **Il vous accompagnera étape par étape pour remplir votre fiche dans le registre des traitements, en vous fournissant des fiches pratiques réparties par grandes catégories et thématiques du RGPD, afin de vous guider de manière claire et progressive**.

Les fiches pratiques ont été conçues pour vous offrir **la même valeur ajoutée que si vous aviez bénéficié de plusieurs séances d'accompagnement avec votre DPO**. Vous pourrez ainsi suivre cette même démarche de manière autonome, à votre rythme, tout en étant guidé par des encarts de couleurs reprenant les bonnes pratiques, les points de vigilance, des focus spécifiques, des exemples concrets, ainsi que des ressources complémentaires pour vous accompagner tout au long du processus.

Le kit de conformité comprend 14 fiches pratiques couvrent, point par point, les **aspects fondamentaux à compléter dans votre fiche de traitement**. Il est recommandé de suivre ces fiches **dans l'ordre**, car elles ont été organisées de manière à offrir une cohérence logique et faciliter la compréhension.
Attention, certaines questions ne nécessitent pas toujours de réponse. Cela sera clairement précisé dans les consignes du kit de conformité, vous pourrez ignorer ces champs. Pour vous aider à repérer rapidement les champs à compléter, ceux-ci seront indiqués **en bleu** et seront également rappelés dans les encarts de conclusion à la fin de chacune des fiches pratiques.

Si, après avoir consulté les fiches, des questions subsistent ou si votre situation nécessite un accompagnement plus spécifique, n'hésitez pas à nous contacter (dpo@univ-paris1.fr). Des échanges par email ou des points de suivi individuels pourront être organisés pour vous apporter une assistance plus personnalisée si le kit de conformité s'est révélé insuffisant.
De plus, **si vous souhaitez une relecture ou un avis sur votre travail après avoir appliqué les conseils du kit de conformité, n'hésitez pas non plus à nous contacter**. Quel que soit l'état d'avancement de votre fiche, nous restons à votre disposition pour vous accompagner.

Gardez à l'esprit que, bien que le DPO conserve votre fiche, il ne pourra généralement pas en assurer un suivi individuel systématique. **Il s'agit d'un travail que vous effectuez en autonomie**, mais sur lequel nous restons bien entendu disponibles pour vous aider si vous en faites la demande.

Bon courage ! 💪

Fiche 1 : Contexte et éléments généraux

Avant de plonger dans le cœur du processus de conformité, il est important de bien débuter en remplissant la fiche de registre de traitement, en fournissant tous les éléments contextuels essentiels pour mieux situer le cadre de votre projet.

Quels sont les éléments généraux que je dois fournir ?

1) Nom du projet de recherche
Commencez par indiquer le nom du projet de recherche pour lequel vous allez travailler sur la conformité RGPD. Ce nom facilitera la recherche future de votre projet dans la liste des fiches du registre de traitement par mot-clé.
Il est recommandé d'inscrire l'intitulé exact (s'il existe) ou le thème principal du projet, de préférence en français. Votre nom/prénom n'est pas requis dans le titre.

⚠️ Attention

Évitez les noms trop génériques, comme « Projet ANR », qui ne vous distingueraient pas des nombreuses autres fiches similaires. De même, évitez les intitulés trop vagues, tels que « Projet ERC Dupont », qui n'apportent pas assez d'informations sur le contenu du projet.

L'objectif est qu'en cas de contrôle par la CNIL (Commission Nationale de l'Informatique et des Libertés), celle-ci puisse avoir une idée générale de chaque projet en consultant simplement les noms des fiches, sans devoir les ouvrir une par une.

📌 Exemples

- « Covid long - Processus de contestation et de stabilisation d'une pathologie émergente »
- « Projet REPREX - Vers une compréhension interdisciplinaire et ascendante des expériences reproductives »

2) Nom du chercheur principal et son laboratoire de rattachement
Dans la section « **Interlocuteur(s)** », indiquez le nom du chercheur principal responsable de la recherche, puis sélectionnez votre structure ou composante de rattachement dans la liste déroulante prévue à cet effet. Si vous travaillez seul, vous serez évidemment cet interlocuteur.

En cas de collaboration, mentionnez uniquement la ou les personnes chargées de la mise en conformité et de la protection des données personnelles (en général, ce n'est pas l'ensemble de l'équipe), ainsi que leurs laboratoires ou structures de rattachement respectifs.

⚠️ Attention

Seules les personnes rattachées à l'université Paris 1 Panthéon-Sorbonne, disposant d'une adresse email en @univ-paris1.fr, peuvent être indiquées dans le champ « interlocuteur ».

🔍 **FOCUS : Pourquoi est-il si important de connaître la structure de rattachement ?**

Le laboratoire est désigné comme « responsable de traitement » au sens du RGPD. Cela signifie qu'il définit les finalités (le pourquoi) du traitement de données ainsi que les moyens utilisés (le comment).

Toutefois, la désignation du responsable de traitement varie selon le type d'unité de recherche :
- Pour les UMR (unités mixtes de recherche), c'est le directeur de l'unité qui est responsable du traitement.
- Pour les autres unités de recherche hors UMR, c'est le président(e) de l'université qui est responsable du traitement.

Plus important encore, c'est le responsable de traitement qui assume la responsabilité des traitements réalisés par ses agents ou chercheurs et, en cas de non-conformité, il en porte les conséquences. Ainsi, une non-conformité majeure entraînant une violation de données de votre part pourrait avoir des répercussions bien au-delà de vos propres travaux, impactant potentiellement votre laboratoire et/ou l'université en cas de sanctions.

3) Domaine applicatif du traitement
Sélectionnez simplement « recherche » dans la liste déroulante. Ce domaine a été défini pour regrouper toutes les fiches des doctorants et chercheurs de l'université.

4) Responsabilité du traitement de données
Les trois champs libres « **Traitement en co-responsabilité** », « **Traitement en tant que sous-traitant** » et « **Détails responsabilités** » visent à préciser si le traitement de données personnelles relève de l'un de ces deux cas.

Si vous réalisez votre projet de recherche seul ou si tous les membres du projet appartiennent à des laboratoires de Paris 1, vous n'avez pas à remplir ces champs et pouvez simplement y inscrire « N/A ».

- Traitement en tant que sous-traitant : Cette situation ne concerne que très peu de chercheurs. Elle s'applique lorsque l'université Paris 1 (ou l'une de ses unités de recherche) est mandatée pour réaliser des travaux de recherche pour le compte d'une tierce personne. Cette relation doit être formalisée par un contrat de prestation stipulant clairement que l'université (et, par extension, le laboratoire et ses chercheurs) agissent en tant que sous-traitants pour le compte d'un tiers. Si tel est votre cas, indiquez « OUI » dans ce champ et précisez l'identité de la personne (physique ou morale) qui sollicite la prestation dans le champ de détail en dessous. Pour tous les autres qui ne sont pas concernés, vous pouvez inscrire « N/A » dans les deux champs.

- Traitement en co-responsabilité : Si vous travaillez dans un projet impliquant plusieurs laboratoires et unités de recherche externes à Paris 1, vous devrez préciser ici que « OUI » vous êtes concerné(e). Dans le champ de détail dessous, indiquez l'ensemble des structures et établissements de rattachement des membres impliqués, en plus de ceux de Paris 1, que vous devrez également mentionner. L'objectif est d'identifier tous les acteurs qui pourraient être conjointement responsables en cas de litige lié à une ingérence des données personnelles dans la gestion du projet.

✅ **Bonne pratique**

Dans le cas d'une recherche multi-tutelle impliquant plusieurs établissements et structures de recherche, sans qu'il y ait de « chercheur principal chef de projet », il est conseillé de désigner une ou deux personnes maximum comme référents RGPD au sein du projet. Ces référents auront pour responsabilité de compléter la fiche présente ici, de promouvoir les bonnes pratiques à suivre et de servir de point de contact privilégié avec le DPO.

🔍 **FOCUS : Pourquoi est-il important de définir les rôles et responsabilités des acteurs du projet ?**

Le RGPD impose diverses responsabilités et obligations aux responsables de traitement et aux sous-traitants. Il est donc essentiel de définir ces rôles dès le début de la recherche :

- Pour rappel, le responsable de traitement détermine les finalités et les moyens du traitement (le « pourquoi » et le « comment » de la recherche). Cela peut être le sponsor de la recherche ou le chercheur lui-même. Dans le cadre d'une recherche au sein d'un consortium, il peut y avoir des responsables conjoints du traitement.

- Un chercheur peut également agir en tant que sous-traitant lorsqu'il réalise des recherches pour le compte d'une entreprise ou d'une autorité, tout en pouvant également lui aussi recourir à d'autres chercheurs comme sous-traitants pour certains aspects d'un projet.

Il est donc crucial, pour chaque projet de recherche, de vérifier comment ces différents rôles doivent être attribués afin que les responsabilités et obligations de chacun soient clairement identifiées et comprises.

5) Déclaration(s) CNIL antérieure(s)

Ce champ se trouve en dessous et correspond à la première question de la section « **Formalités** » suivante. Il est destiné aux personnes ayant débuté leurs travaux avant 2018, date à laquelle le RGPD est entré en vigueur, et qui devaient alors contacter la CNIL pour déclarer les traitements réalisés avec les données. Si cela vous concerne, merci d'indiquer la date à laquelle vous avez contacté la CNIL, de fournir quelques précisions sur le dossier que vous leur avez soumis et, si possible, le numéro de référence de votre déclaration antérieure.
Notez cependant que ce système est désormais révolu, et la seule formalité actuelle consiste à remplir cette fiche du registre des traitements.

Si vous n'avez pas commencé vos travaux avant 2018 ou si vous n'aviez pas effectué de déclaration auprès de la CNIL à ce moment-là, vous n'êtes pas concerné et pouvez simplement indiquer « N/A ».

6) Mise à jour du traitement

En bas de la page du registre, vous trouverez une section « **Mise à jour du traitement** » avec deux champs à remplir :
- « **Date de mise en œuvre** » : Indiquez la date de début de votre projet de recherche, si vous la connaissez. Il s'agit de la date où le projet a véritablement commencé, notamment avec la réflexion méthodologique, et non celle du début de collecte et de traitement des données.
- « **Date fin de traitement prévue** » : Indiquez ici la date de clôture du projet. Pour un projet financé, cette date coïncide souvent avec la fin du financement. Sinon, il peut s'agir de la date de publication du livrable final.

Si vous n'avez pas les dates exactes, ce n'est pas problématique. Faites de votre mieux pour indiquer une estimation réaliste. En cas d'incertitude, vous pouvez inscrire le premier ou dernier jour d'un mois ou d'une année.

Quant au champ « **Mise à jour traitement** », il est facultatif. Vous pouvez l'ignorer, sauf si vous souhaitez connaître la date et l'heure de votre dernière modification. Sans le remplir, vous verrez la date de création de la fiche et le nombre total de mises à jour effectuées, mais pas la date de la dernière modification.

7) Documentation et Remarques
Au bas de la page, vous trouverez une section « **Documentation** », où vous pouvez ajouter autant de documents en annexe que nécessaire. Avant de commencer votre processus de mise en conformité, il est souvent recommandé d'y joindre votre méthodologie ou protocole de recherche, si vous en avez déjà un. Ce document contient généralement des informations précieuses qui vous aideront à remplir votre fiche RGPD.

Par la suite, vous pourrez ajouter d'autres documents de votre choix que vous n'avez pas pu inclure dans d'autres sections.

Concernant les champs « **Bloc-notes** » et « **Commentaires** » dans la section « **Remarques** », il n'est pas nécessaire de les utiliser. Vous pouvez simplement les ignorer.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de remplir les champs suivants dans votre fiche du registre des traitements :
- **Nom du traitement**
- **Structure(s) / composante(s)**
- **Interlocuteur(s)**
- **Domaine applicatif du traitement**
- Indication si le **traitement est en co-responsabilité**, en **sous-traitance**, ainsi que les **détails des responsabilités** le cas échéant
- **Déclaration(s) CNIL antérieure(s)**
- **Mise à jour traitement**, ainsi que la date de **Date de mise en œuvre** et **Date fin de traitement prévue**
- **Documentation**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 2 : Les finalités du traitement de données

Qu'est-ce qu'une finalité de traitement ?

Les finalités de traitement désignent les objectifs pour lesquels des données personnelles sont traitées. En d'autres termes, **c'est la raison pour laquelle vous avez besoin de ces données**.
L'objectif de cette fiche est de vous permettre de décrire clairement les **objectifs poursuivis** par le traitement des données personnelles dans le cadre de vos recherches. En d'autres termes, vous devez expliquer pourquoi vous avez besoin de collecter ces données. Par exemple l'amélioration de tel algorithme, l'analyse de tel phénomène démographique etc.

Comment identifier mes finalités de recherche ?

Voici les principales questions à vous poser pour vous aider :
- Quel est l'objectif principal de ma recherche ? Décrivez le but global de votre étude.
- Pourquoi ai-je besoin de collecter ces données spécifiques ? Identifiez les raisons précises pour lesquelles chaque type de donnée est nécessaire.
- Comment ces données contribueront-elles à la réalisation de mon projet ? Expliquez le lien entre les données collectées et les résultats attendus de votre recherche.
- Quelles hypothèses ou questions de recherche est-ce que je souhaite explorer grâce à ces données ? Précisez les questions scientifiques ou hypothèses que vous souhaitez vérifier.

A noter qu'il peut y avoir une finalité principale et des finalités secondaires, si cela est pertinent (par exemple, l'élaboration de statistiques à partir des données recueillies, ou l'exploration d'axes de recherche secondaires).

Que dois-je indiquer dans la fiche du registre ?

Une fois vos finalités identifiées, il vous suffira de compléter le champ « **Finalité** » dans la section « **Formalités** » par une description succincte et concise de votre projet de recherche. L'objectif est de résumer en quelques lignes l'idée générale de votre étude.
Dans le champ « **Détails des finalités** », vous pourrez développer davantage l'objectif de votre recherche, mentionner d'éventuelles sous-finalités, ainsi que les projets que vous envisagez de réaliser avec les données. Ce champ est destiné à inclure les réponses aux questions précédentes.

Lorsque vous décrivez les finalités du traitement des données, assurez-vous qu'elles respectent les trois critères suivants :
- **Spécifiques** : Les finalités doivent être clairement définies et précises, afin que l'on comprenne exactement pourquoi les données sont collectées.
- **Explicites** : Elles doivent être formulées de manière claire et compréhensible, pour que les personnes concernées sachent comment leurs données seront utilisées. Utilisez des termes simples et accessibles. Assurez-vous que les finalités soient compréhensibles par tous, y compris ceux qui ne sont pas spécialistes de votre domaine.
- **Légitimes** : Elles doivent être justifiées et conformes aux lois, sans porter atteinte aux droits des personnes concernées.

📌 Exemples

Finalité
Le projet vise à analyser la circulation du concept de justice reproductive et les transformations qu'il subit. Dans le cadre du projet ERC, il s'agit d'examiner comment les femmes se positionnent, consciemment ou non, dans une double perspective à la fois verticale (politique, juridique et conceptuelle) et horizontale (intime et sociale), et l'impact de cette position sur leurs décisions reproductives.

Détails de la finalité
- Une enquête ethnologique, sociale et démographique sera menée. Elle inclut l'interrogation de groupes de femmes aux horizons divers afin de comprendre leurs perceptions et expériences concernant les liens entre droits reproductifs, justice reproductive et gouvernance reproductive.
- Un site sera développé pour présenter des informations sur le projet et l'équipe, ainsi que publier régulièrement des billets sur l'actualité du projet (comme des colloques).
- Un podcast sera produit et probablement diffusé sur le site internet mentionné ci-dessus. Ce podcast inclura des lectures d'extraits ou de passages de certains entretiens ou interviews.

⚠️ Attention

Certaines raisons pour lesquelles vous collectez et utilisez des données personnelles nécessitent une **évaluation approfondie des risques pour la vie privée**, appelée AIPD (Analyse d'Impact sur la Protection des Données). Veuillez consulter la fiche 14 pour plus de détails.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Finalité**
- **Détails des finalités**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 3 : Base légale de traitement

Qu'est-ce qu'une base légale ?

Pour pouvoir être mis en œuvre, tout traitement de données personnelles doit reposer sur l'une des bases légales prévues par le RGPD. La base légale d'un traitement est **le fondement juridique qui autorise et justifie le traitement des données personnelles**. Ce choix de la base légale doit intervenir avant la mise en œuvre du traitement des données. En l'absence de base légale, le traitement ne pourra pas être mis en œuvre : il ne sera donc pas possible de collecter, d'utiliser ou de réutiliser des données.

Quelles bases légales existe-il ?

Le RGPD prévoit six bases légales permettant de justifier un traitement de données personnelles. Parmi elles, deux sont principalement adaptées aux traitements de données réalisés dans le cadre de la recherche scientifique. Il est essentiel de choisir la base légale la plus pertinente, en fonction des objectifs de la recherche et des spécificités du traitement envisagé :

- **L'exécution d'une mission d'intérêt public** (ou relevant de l'exercice de l'autorité publique) : Cette base légale concerne en premier lieu les traitements mis en œuvre par les autorités publiques et les organismes publics (comme les universités) dans le cadre de leur mission statutaire. Cette base légale sera privilégiée dès lors que le chercheur pourra démontrer l'intérêt public de ses recherches.
Par exemple, une recherche en sociologie avec collecte de messages échangés sur Twitter peut avoir pour fondement la mission d'intérêt public.

- **Le consentement de la personne concernée** : Lorsque vous avez obtenu l'accord clair et explicite de la personne pour traiter ses données. Par exemple, les enquêtes de terrain en France se réalisent souvent sur le fondement d'un consentement donné à l'enquêteur.

✅ Bonnes pratiques

- Le consentement doit être donné par une déclaration ou tout autre acte positif clair. La réglementation n'impose donc pas de modalité particulière pour recueillir le consentement, mais il faudra toutefois que le responsable de traitement soit en mesure de démontrer sa validité.

- Les consentements recueillis au moyen d'une case pré-cochée ou les consentements « groupés » (un seul consentement demandé pour plusieurs traitements distincts) pour des recherches en réalité indépendantes ne sont pas considérés comme valables.

- Le consentement du mineur seul, même après 15 ans, n'est pas valable pour une recherche scientifique. C'est le consentement des titulaires de l'autorité parentale qui doit être recueilli.

⚠ Attention

Le consentement est envisagé au sens de la réglementation en matière de protection des données et non de l'accord qui peut être donné par les participants à une recherche. Lorsque le consentement est la base légale de la recherche, la personne interrogée doit donner un consentement spécifique au traitement de ses données personnelles. Il est ainsi nécessaire d'utiliser dans le formulaire deux cases distinctes, l'une pour recueillir le consentement RGPD, l'autre pour participer à la recherche.

Une recherche non fondée sur la base légale du consentement mais sur un motif d'intérêt public peut néanmoins nécessiter l'accord des personnes concernées pour participer à la recherche.

Si aucune de ces bases légales ne semble correspondre à votre situation, n'hésitez pas à consulter votre DPO pour explorer d'autres bases légales possibles.

Quelles bases légales dois-je utiliser ?

En pratique, vous constaterez rapidement que, dans le cadre de travaux de recherche, vous serez souvent tenté d'utiliser soit le consentement de la personne, soit la mission d'intérêt public comme base légale.

Pour que le consentement soit libre, il ne doit pas exister de déséquilibre manifeste des rapports de force entre le responsable de traitement et la personne concernée. En ce sens, le considérant 43 du RGPD interdit à une institution publique ou un employeur de se fonder sur le consentement comme base légale [1]. Cela s'explique par le fait que le consentement, lorsqu'il est sollicité par une autorité publique, pourrait ne pas être considéré comme librement donné, en raison du rapport de pouvoir inhérent à la relation entre l'autorité et les individus. En d'autres termes, les personnes pourraient se sentir obligées de consentir, ce qui compromettrait la validité de ce consentement. Il peut exceptionnellement être toléré lorsqu'il est possible de veiller à ce qu'il soit libre, c'est-à-dire que la personne concernée puisse refuser de le donner sans subir de conséquence négative.

Étant donné que l'université est considérée comme une autorité publique, cette restriction s'applique également à Paris 1. C'est pourquoi, dans la majorité des cas, **vous devrez utiliser la mission d'intérêt public** (ou émanent d'une autorité publique) comme base légale **en expliquant en quoi vos recherches et votre projet scientifique contribuent à l'intérêt public** (votre statut de chercheur n'étant pas suffisant pour garantir l'utilisation de la mission d'intérêt public).

⚠ Attention

Bien que l'exécution d'une mission d'intérêt public soit généralement la base légale retenue dans le registre, et que l'article 89(1) vous permette de déroger à l'obligation de consentement dans le cadre de vos travaux pour ce motif, il est fortement recommandé d'obtenir le consentement

[1] Les lignes directrices du Comité Européen de la Protection des Données (CEPD) déconseillent fortement aux autorités publiques d'utiliser le consentement comme base légale en raison du déséquilibre de pouvoir.

explicite et éclairé des participants à ce que vous traitiez leurs données personnelles dans le cadre de vos recherches, comme mesure de précaution supplémentaire.

Que dois-je indiquer dans la fiche du registre ?

Comme indiqué, dans la section « **Formalités** », vous trouverez un champ intitulé « **Base juridique** » où vous pourrez sélectionner « mission d'intérêt public (article 6-1e) » à partir de la liste déroulante.

Dans le champ du dessous, nommé « **Détail base juridique** », je vous invite à ajouter les éléments suivants en complétant les informations entre crochets avec celles de votre projet de recherche :
« *L'article L. 711-1 du code de l'éducation détermine que "Les établissements publics à caractère scientifique, culturel et professionnel [...] sont pluridisciplinaires et rassemblent des enseignants-chercheurs, des enseignants et des chercheurs de différentes spécialités afin d'assurer le progrès de la connaissance", ainsi que sur l'article L. 123-3 du même code qui indique que "Les missions de service public de l'enseignement supérieur sont [...] la recherche scientifique et technologique, la diffusion et la valorisation de ses résultats au service de la société.".*
Au fondement de ces deux dispositions, l'université poursuit une mission de recherche scientifique.

La collecte des données dans le cadre du projet de recherche ***[insérer nom du projet]*** *s'inscrit par conséquent dans cette mission de recherche dévolue à l'université et est nécessaire au regard des objectifs poursuivis par le projet, notamment en ce qu'il doit permettre de* ***[indiquer l'intérêt public de votre projet]***. »

Le cas échéant, si concerné(e), vous pouvez également préciser : « *En complément de cette base légale, le consentement des participants sera systématiquement recueilli, garantissant ainsi qu'ils sont pleinement informés et qu'ils acceptent volontairement de contribuer à la recherche.* »

📌 **Exemple de justification de l'intérêt public d'un projet**

Ce projet d'étude sur la justice reproductive est d'intérêt public car il génère des connaissances essentielles qui impactent directement la société. En analysant la circulation et les transformations du concept de justice reproductive, il fournit des données cruciales pour informer et orienter les politiques publiques et les pratiques médicales. Ces résultats peuvent influencer les législateurs, en leur offrant des preuves solides pour élaborer ou ajuster des lois relatives à la santé reproductive et aux droits humains.

🎯 **Récapitulatif**

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Base juridique**
- **Détails base juridique**

Si ce n’est pas le cas ou si vous avez des questions, n’hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 4 : Personnes concernées

Qui sont les "personnes concernées" ?

Dans le cadre du RGPD, les "personnes concernées" désignent les individus dont les données personnelles sont collectées, traitées et utilisées. Autrement dit, celles qui **fournissent leurs informations personnelles dans le cadre de vos recherches**.

L'article 30(1)(c) du RGPD vous oblige à **déterminer qui sont les personnes concernées** dans le cadre de votre recherche. Cela peut inclure des participants à des enquêtes, des interviewés, des patients, des étudiants, etc. Il faut donc que vous ayez la capacité de pouvoir identifier les catégories des personnes concernées, leur nombre approximatif etc.

Comment identifier les personnes concernées ?

- **Définir l'objet de votre recherche** : Commencez par clarifier les objectifs de votre recherche. Quel est le but de la collecte des données et quel type d'informations recherchez-vous ? Par exemple, si vous réalisez une étude sur les habitudes alimentaires, vos personnes concernées seront celles dont vous collectez des données alimentaires.

- **Identifier les sources de données** : Déterminez d'où proviendront vos données. S'agit-il de participants à des enquêtes, d'interviewés, de patients, d'étudiants, de membres d'une organisation, ou d'autres groupes ? La source de vos données vous aidera à définir qui sont les personnes concernées.

- **Préciser les critères de sélection** : Établissez les critères spécifiques qui définissent les personnes que vous incluez dans votre recherche. Par exemple, si vous enquêtez sur les habitudes de lecture des adolescents, vos personnes concernées seront des adolescents répondant à des critères d'âge spécifique.

Que dois-je indiquer dans la fiche du registre ?

Dans la section « **Formalités** », vous trouverez plusieurs champs dédiés aux personnes concernées. Commencez par sélectionner les « **Catégories des personnes concernées par le traitement** » dans la liste déroulante, en choisissant celles qui se rapprochent le plus des groupes que vous avez identifiés. Ajoutez autant de champs que nécessaire.

Ensuite, dans le champ « **Autres personnes concernées** », décrivez de manière détaillée votre analyse en listant de façon exhaustive les personnes concernées. Vous pouvez également y préciser les critères de sélection et de définition de ces personnes, si disponibles.

Enfin, dans le champ « **Nombre approximatif de personnes concernées** » situé plus bas, indiquez une estimation du nombre de personnes identifiées (un nombre approximatif suffit pour donner un ordre d'idée). Vous pouvez ajouter des précisions supplémentaires si nécessaire.

📌 Exemples

Catégories de personnes concernées : Les personnes concernées par le projet de recherche sur la justice reproductive se répartissent en deux groupes principaux. D'une part, les praticiens et universitaires, tels que les gynécologues, médecins, et chercheurs, qui participeront aux entretiens informationnels. D'autre part, les femmes majeures qui prendront part aux entretiens individuels socio-ethnographiques. Ces deux catégories permettent de recueillir des perspectives diverses et complémentaires sur les enjeux de la justice reproductive, notamment dans le contexte des pratiques et des vécus individuels.

Nombre approximatif de personnes : Quant au nombre de personnes impliquées, environ 100 à 130 individus sont concernés par le traitement des données. Parmi eux, 20 à 30 participeront aux entretiens informationnels, tandis que 80 à 100 seront engagés dans des entretiens individuels.

✅ Bonnes pratiques

Le lecteur de votre fiche de traitement, qu'il s'agisse de la CNIL ou du DPO, n'a pas connaissance des spécificités de vos recherches. Ce qui peut vous sembler évident ne l'est pas nécessairement pour eux. Il est donc recommandé de justifier brièvement, en une à deux phrases, la nécessité de traiter les données de chaque catégorie de personnes concernées et de faire appel à elles, surtout si cette raison n'apparaît pas de manière évidente.

Par exemple :
- Femmes majeures participant aux entretiens individuels socio-ethnographiques : Les données collectées auprès de ces femmes sont essentielles pour analyser et comprendre leurs expériences et perceptions sur la justice reproductive.
- Gynécologues participant aux entretiens informationnels : Les entretiens avec des gynécologues et autres praticiens apportent des connaissances clés sur les pratiques médicales et les défis rencontrés dans le domaine de la justice reproductive.

⚠️ Attention

Si votre recherche implique des mineurs ou des personnes vulnérables parmi les personnes concernées, il est essentiel de suivre des procédures supplémentaires pour garantir leur protection. N'hésitez pas à prendre contact avec votre DPO pour vous faire aider (dpo@univ-paris1.fr).

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Catégories des personnes concernées par le traitement**
- **Autres personnes concernées (détails des personnes concernées)**
- **Nombre approximatif de personnes concernées**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 5 : Données personnelles traitées

Qu'est-ce qu'une donnée personnelle ?

Les données personnelles sont **toutes les informations** liées à une personne physique identifiée ou identifiable. Autrement dit, toute donnée permettant, **seule ou combinée** à d'autres informations, d'identifier une personne est considérée comme personnelle.

Dans le cas de l'identification directe, on peut reconnaître une personne immédiatement à partir d'une information unique, comme un nom ou un numéro de sécurité sociale ; ici, le caractère personnel de la donnée est évident.
En revanche, une identification indirecte, nécessitant la combinaison de plusieurs informations (par exemple, l'âge, la ville et la profession) permettant de retrouver une personne sans la nommer explicitement, constitue aussi des données personnelles, bien que cela soit parfois moins évident.

Comment déterminer si vous traitez des données personnelles ?

Passez en revue les types de données que vous collectez. Sont-elles liées à des individus et peuvent-elles être utilisées pour les identifier ? Si oui, elles sont considérées comme des données personnelles.
Parfois des données seules ne sont pas identifiantes directement - comme la profession de la personne -, mais si elles sont associées à une autre donnée - comme le nom du service où elle travaille - elles peuvent le devenir.

📌 Exemple

Appliqué au domaine de la recherche, le traitement de données peut prendre plusieurs formes : il peut s'agir par exemple d'une base de données (avec le nom ou un numéro permettant d'identifier une personne), d'un fichier papier ou numérique, de l'enregistrement oral ou du script d'un entretien mené dans le cadre d'une recherche en sociologie, de notes prises sur un carnet dans le cadre d'une recherche en psychologie, de photographies prises pour une recherche en ethnographie, d'un enregistrement audiovisuel dans le cadre d'un projet de recherche en sciences du langage, d'une application mobile, de dispositifs biométriques utilisés pour le développement d'une technologie, etc.

⚠️ Attention

Vous pensez ne pas traiter de données personnelles ? C'est un postulat qui s'avère faux dans 90% des cas, car la notion de "donnée personnelle" est extrêmement large. Les données personnelles sont quasiment toujours là, même quand on ne les attend pas !
En effet, même si certaines informations ne semblent pas immédiatement personnelles, leur combinaison avec d'autres bases de données permet généralement d'identifier les personnes.
En cas de doute, n'hésitez pas à contacter votre DPO pour confirmation.

L'article 30(1)(c) du RGPD exige que **vous listiez précisément les catégories de données personnelles que vous utilisez**. Il est essentiel de consacrer du temps à dresser une liste exhaustive de toutes les données que vous collectez ou envisagez de collecter. Pour vous guider dans cette démarche, voici une liste des types de données les plus couramment traitées dans les recherches :

- Informations d'identification : Nom, prénom, image, date de naissance, genre…
- Coordonnées : Adresse postale, numéro de téléphone, adresse e-mail…
- Vie personnelle : Habitudes de vie, situation familiale…
- Vie professionnelle : Situation professionnelle, scolarité, formation, diplômes…
- Données comportementales : Préférences, habitudes de consommation, goûts…
- Données de connexion : Adresses IP, logs, identifiants, informations d'horodatage, cookies…
- Données sensibles (cf. point d'attention ci-dessous) : Opinions politiques, croyances religieuses, orientation sexuelle, origine ethnique ou raciale et données de santé.

Etc…

📌 Exemple

Dans le cadre d'une recherche sur la justice reproductive, le responsable de traitement a déclaré avoir collecté l'ensemble des informations suivantes :

- Informations de contact, telles que l'adresse e-mail, pour permettre la communication sur l'évolution du projet et les résultats obtenus grâce à la participation des enquêtés.
- Données d'identification personnelles : nom, prénom, année de naissance, genre.
- Catégorie socio-professionnelle et trajectoire sociale (linéaire ou non, ruptures, etc.).
- Pays de l'entretien et indication si la personne réside en zone urbaine, périurbaine ou rurale.

Pour les entretiens informationnels :

- Profession, tâches ou missions professionnelles exercées.
- Rattachement institutionnel (institution médicale, juridique, universitaire, etc.).
- Éventuelles interventions publiques mentionnées, comme des prises de parole dans les médias ou les institutions parlementaires.

Pour les entretiens socio-ethnographiques :

- Indicateur géographique de la résidence principale pour évaluer l'accès aux services de santé sexuelle et reproductive.
- Catégorie socio-professionnelle.
- Données spécifiques à l'enquête, incluant le nombre d'enfants (ou non), d'accouchements, d'avortements, de fausses couches, éventuelles expériences de violences sexuelles, gynécologiques ou obstétricales, interactions avec les services sociaux ou de protection de l'enfance, sexualité, rapport à la maternité et à la parentalité, allaitement, questions menstruelles, ménopause, et positionnement par rapport à l'engagement féministe.

⚠️ Attention

La collecte de données dites sensibles, est strictement encadrée par l'article 9 du RGPD. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou

l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).
De plus, une donnée a priori non sensible peut toutefois le devenir en cas de recoupement d'informations. Par exemple, des recherches portant sur la géolocalisation des véhicules pourraient révéler des convictions politiques réelles ou supposées, des convictions religieuses et/ou des données relatives à la santé par l'étude des habitudes de déplacement et du stationnement sur le parking de lieux particuliers (locaux d'un parti politique, fréquentation de lieux de culte, etc.).

En principe, le traitement des données sensibles est interdit. Toutefois, il peut être **exceptionnellement autorisé dans le cadre de vos recherches** selon l'article 9(2) du RGPD dans l'un des cas suivants :
- Si la personne concernée a donné son consentement explicite pour le traitement de ces données.
- Si les données sensibles ont été manifestement rendues publiques par la personne concernée.
- Si le traitement est nécessaire à des fins de recherche scientifique, historique ou statistique, conformément à l'article 89(1) [2], à condition de mettre en place des mesures de sécurité appropriées.

Pour toutes ces catégories particulières de données, n'hésitez pas à prendre contact avec votre DPO.

La collecte de données personnelles peut se faire de plusieurs façons :
- **Directement auprès des personnes concernées**, **par vous-même ou un membre de l'équipe de recherche** : cela inclut des méthodes comme les questionnaires, formulaires, enquêtes, entretiens (semi-directifs, directifs) ou expériences en laboratoire. Ces données peuvent être recueillies sous divers formats : texte, image, audio, vidéo. Quelle que soit leur forme, elles sont toutes soumises au RGPD.

- **Directement par un prestataire ou sous-traitant au nom du chercheur** : si vous déléguez la collecte de données à un tiers dans le cadre de votre recherche, ce dernier doit garantir la sécurité et la confidentialité des données. Un contrat de sous-traitance conforme à l'article 28 du RGPD doit obligatoirement être signé.

- **Indirectement, par la réutilisation de données existantes ou collectées par un tiers** (hors prestataire) : cela peut concerner des bases de données déjà utilisées dans d'autres recherches, des données accessibles publiquement sur internet ou des demandes d'accès à des données auprès de centres spécialisés, comme le CASD.

[2] Cet article précise les conditions dans lesquelles les données sensibles peuvent être traitées pour des objectifs de recherche scientifique ou historique, ou à des fins statistiques. Il stipule que :
- Le traitement doit être proportionné aux objectifs poursuivis.
- Il doit respecter l'essence du droit à la protection des données.
- Des mesures appropriées et spécifiques doivent être mises en place pour sauvegarder les droits et les intérêts des personnes concernées.

⚠️ Attention

Même si vous ne collectez pas directement les données personnelles, mais réutilisez des données déjà collectées par un tiers, ces données restent pleinement soumises au RGPD.

Dans ce cadre, vous devez impérativement :
- Préciser l'origine de la base de données : il est important d'indiquer si les données proviennent d'une source publique (par exemple, une base de données mise à disposition par une institution publique) ou d'un tiers privé.
- Vérifier la légitimité de la réutilisation : si les données ne sont pas publiques, vous devez démontrer que vous les avez obtenues légalement. Cela peut inclure la signature d'un contrat de partage de données ou encore une convention définissant les conditions d'accès et d'usage des données.
- Vous assurer que les données ont été initialement collectées dans le respect des principes du RGPD, notamment en ce qui concerne l'information et le consentement des personnes concernées, si cela était requis au moment de la collecte. Il pourra également être nécessaire, en fonction des circonstances, d'informer à nouveau les personnes concernées de la réutilisation de leurs données dans le cadre de votre nouvelle finalité de recherche.

🔍 FOCUS : La réutilisation de données rendues publiques

Même si les données personnelles utilisées dans le cadre de votre recherche sont manifestement rendues publiques par les individus eux-mêmes (par exemple, dans des films, séries, clips ou publicités), vous restez soumis au RGPD. Toutefois, certaines exigences peuvent être allégées :

- Vous pouvez vous appuyer sur la mission d'intérêt public comme base légale pour le traitement, ce qui simplifie les formalités liées au consentement des personnes concernées (cf. fiche 3).

- Vous pourriez être exempté de fournir la mention d'information habituelle aux individus, notamment concernant leurs droits d'accès et de rectification, étant donné que les données sont largement accessibles au public (cf. fiche 8). Il est donc raisonnable de considérer que les personnes concernées sont informées de l'utilisation potentielle de leurs données.

- Certains droits des personnes concernées, tels que le droit d'opposition ou le droit à l'effacement, pourraient être allégés. Cependant, pour limiter les risques, il est recommandé de diffuser une information générale précisant que les personnes dont les données sont utilisées peuvent se manifester si elles se reconnaissent dans les œuvres traitées et souhaitent ne pas voir leurs données collectées pour la recherche. Si nécessaire et après vérification de leur identité, elles pourraient être retirées de l'étude (cf. fiche 7).

Si vous êtes concerné par cette situation, n'hésitez pas à contacter votre DPO.

🔍 FOCUS : Principe de proportionnalité et de minimisation

Selon l'article 5(1)(c) du RGPD, vous devez **uniquement collecter et traiter les données personnelles nécessaires pour atteindre les objectifs de votre recherche**. En d'autres termes, chaque donnée collectée doit être strictement nécessaire et justifiée par les objectifs de votre recherche. Évitez de recueillir des informations « au cas où » sans nécessité concrète. Si possible, essayez de vous passer des données personnelles.

Il est donc essentiel de déterminer à l'avance quelles données sont réellement nécessaires pour votre recherche. Ainsi, vous pourrez vous assurer de ne collecter que ces informations spécifiques et, le cas échéant, supprimer toute donnée supplémentaire que vous auriez pu obtenir.

Voici quelques exemples de questions à se poser lors de la définition des données à collecter dans le cadre de votre traitement :
- Âge : La collecte de l'âge exact est-elle indispensable ? Peut-être qu'une simple tranche d'âge serait suffisante pour répondre aux objectifs de la recherche ?
- Lieu de résidence : Avez-vous réellement besoin de connaître l'adresse complète des participants ou la ville de résidence suffit-elle ?
- Activité professionnelle : Est-il nécessaire de recueillir le métier exact exercé par les participants ou une simple mention de la catégorie socio-professionnelle serait-elle suffisante ?
Etc...

🔍 **FOCUS : Est-il possible de traiter des données personnelles de personnes décédées ?**

Les droits Informatique et Libertés sont des droits personnels qui disparaissent avec le décès de la personne. Toutefois, la loi Informatique et Libertés prévoit la possibilité pour une personne de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données personnelles après son décès.
Par ailleurs, la CNIL recommande d'appliquer les règles relatives à la protection des données lorsque le traitement des données de personnes décédées est susceptible d'avoir des conséquences sur la vie privée de leurs ayants droits ou de proches.

Comment dois-je remplir la fiche du registre ?

Une fois toutes les données personnelles identifiées, vous pourrez les consigner dans la fiche du registre. Dans la catégorie « Données traitées », commencez par renseigner le champ « **Données identifiantes (directes et indirectes)** » en détaillant toutes les données personnelles. Si cela vous est plus clair, vous pouvez choisir de distinguer visuellement les données d'identification directe de celles d'identification indirecte.

De plus, si votre projet implique le traitement de données sensibles (voir la liste ci-dessus), veuillez répondre « OUI » à la question « Données sensibles ? » et les décrire en détail dans le champ approprié « **Détail données sensibles** ». Pour justifier l'utilisation de ces données particulières, il est conseillé d'ajouter une ou deux phrases expliquant leur nécessité dans le cadre de vos travaux, la raison pour laquelle leur collecte est indispensable et de prendre contact avec votre DPO à l'adresse suivante : dpo@univ-paris1.fr

Les champs « **Autres données non identifiantes** », « **Interconnexion de fichier** » et « **Zone de libre commentaire** » ne nécessitent aucune réponse supplémentaire de votre part. Si vous avez bien complété le champ ci-dessus, vous pouvez simplement y inscrire « N/A ».

Enfin, en plus de répertorier toutes les données personnelles collectées, vous devez également préciser la « **Méthode de collecte des données** » dans le champ correspondant. Voici les informations que vous pouvez préciser :

- **Méthode de collecte** : Indiquez si les données ont été recueillies directement auprès des personnes concernées par vous-même ou un membre de votre équipe, par l'intermédiaire d'un prestataire, ou indirectement via une autre source.
- **Supports et formats utilisés** : Mentionnez les supports ou formats selon la nature des données collectées : entretiens (audio, vidéo, transcrits), enquêtes (en ligne, papier), recherches documentaires, exploitation de bases de données existantes, etc.
- **Critères de sélection des participants** : Si votre projet de recherche impose des critères de sélection spécifiques, comme l'âge, le milieu socioculturel, le niveau d'éducation, la nationalité ou l'implication dans un phénomène donné, détaillez-les. Ces éléments sont importants pour justifier la pertinence des données collectées au regard de vos objectifs scientifiques.
- **Modalités de premier contact** : Si vous avez sollicité des personnes pour participer à votre projet, décrivez la méthode utilisée pour établir ce premier contact. Indiquez comment vous avez obtenu leurs coordonnées (par exemple : annuaire public, recommandation, participation volontaire) et précisez la source de ces informations.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Méthode de collecte des données**
- **Données identifiantes (directe et indirecte)**
- **Autres données non identifiantes**
- **Interconnexion de fichiers**
- **Zone de libre commentaire**
- **Données sensibles ?**
- **Détail données sensibles**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 6 : Destinataires des données

Qui sont les destinataires des données ?

Les destinataires des données sont les personnes, organisations ou entités à qui vous communiquez ou partagez les données personnelles que vous avez collectées dans le cadre de vos recherches. Ces destinataires peuvent être internes ou externes à votre institution.

- **Destinataires internes** : Ce sont les membres de votre équipe de recherche, les départements de votre institution ou les autres unités qui nécessitent l'accès aux données pour les besoins de votre projet.
- **Destinataires externes** : Il peut s'agir de partenaires de recherche, d'institutions collaboratrices, d'organismes de financement, des membres d'un comité scientifique chargé d'une revue scientifique peuvent être amenés à avoir communication de certaines données afin de valider les résultats de la recherche, soit pour des analyses, soit pour des publications, etc.

Comment identifier les destinataires de mon traitement ?

L'article 30(1)(d) du RGPD vous oblige à identifier les destinataires des données. Pour ce faire, il suffit de vous poser la question suivante : « Qui aura accès aux données dans le cadre de ce projet ? A qui vais-je les partager ? ».
Il est important de dresser une liste exhaustive des personnes ou entités qui auront besoin d'accéder aux données pour mener à bien votre recherche, en veillant à inclure à la fois les destinataires internes et externes, qu'ils soient présents au sein de l'UE ou en dehors.

Il est à noter qu'une fois que vos travaux de recherche sont terminés et que les résultats agrégés ont été publiés, les données ne sont plus considérées comme des données personnelles au sens du RGPD. Les destinataires concernent uniquement les personnes ayant accès aux données « brutes » avant leur anonymisation.

⚠ Attention

Conformément au principe de minimisation des données, tel qu'énoncé à l'article 5(1)(c) du RGPD, l'accès aux données doit être réservé uniquement aux personnes ayant un besoin légitime d'y accéder. Il est donc crucial de restreindre le nombre de destinataires des données au minimum nécessaire pour le projet, ce qui contribue à réduire les risques pour la confidentialité des informations.

Comment dois-je remplir la fiche du registre ?

Dans la section « **Destinataires des données** », une fois que vous avez identifié vos destinataires, je vous recommande de les organiser en deux groupes distincts :
- Destinataires internes à l'Université Paris 1 : Indiquez-les sous « **Catégories des destinataires internes** » en sélectionnant leur profil dans la liste déroulante.
- Destinataires externes à l'Université Paris 1 : Suivez le même processus dans la section « **Destinataires externes** ».
N'oubliez pas que vous pouvez ajouter autant de catégories que nécessaire.

De la même manière que pour les personnes concernées (cf. fiche pratique 4), si vous avez des difficultés à dresser une liste exhaustive des destinataires, il est acceptable de mentionner simplement les grandes catégories ou les critères qui vous permettent de les identifier.

📌 Exemples

Dans le cadre d'un projet de recherche, les destinataires internes du projet incluent :
- Le chercheur et son équipe de X post-doctorants qui contribueront à la recherche.
- Des vacataires internes chargés de la retranscription de fichiers audio des entretiens.
- Les laboratoires partenaires impliqués dans le projet (à lister).

Les destinataires externes du projet incluent quant à eux :
- Des vacataires externes pour la retranscription des fichiers audio des entretiens.
- Des collaborations avec d'autres chercheurs et chercheuses universitaires.
- Pendant les séminaires collectifs, étant donné leur nature publique, toutes les personnes présentes physiquement ainsi que tous les internautes consultant la rediffusion en ligne peuvent être considérés comme des destinataires.
- Un sous-traitant engagé dans le cadre d'une prestation de création de site internet.

✅ Bonne pratique

Il est recommandé, pour tous les destinataires ayant un accès régulier aux données (qu'ils soient internes ou externes au projet), de leur **faire signer un engagement de confidentialité** et d'en conserver précieusement un exemplaire. Pour vous aider, vous pouvez vous référer à celui joint en ANNEXE 1 : LIEN ICI.

Résumé : À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Catégories de destinataires internes**
- **Destinataires externes**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 7 : Gestion des demandes d'exercice de droit des personnes concernées

Pour rappel (cf. fiche pratique 4), les personnes concernées sont les individus dont les données personnelles sont collectées, utilisées ou traitées dans le cadre de votre recherche. Les articles 12 à 22 du RGPD leur confère plusieurs droits concernant le traitement de leurs données, afin de garantir leur protection et leur contrôle sur ces informations.

Quels sont les principaux droits des personnes concernées ?

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 :

Droit d'accès : Les personnes concernées ont le droit de savoir si leurs données sont traitées, d'accéder à ces données, et d'obtenir des informations sur la finalité du traitement, les catégories de données concernées, et les destinataires de ces données.

Droit de rectification : Elles peuvent demander la correction de données inexactes ou incomplètes les concernant.

Droit à l'effacement / droit à l'oubli : Elles peuvent demander la suppression de leurs données sous certaines conditions.

Droit à la limitation du traitement : Elles peuvent demander la suspension du traitement de leurs données, par exemple pendant que la véracité des données est vérifiée.

Droit à la portabilité des données : Elles peuvent obtenir leurs données dans un format structuré, couramment utilisé et lisible par machine, et demander que ces données soient transférées à un autre responsable du traitement.

Droit d'opposition : Elles peuvent s'opposer au traitement de leurs données pour des raisons tenant à leur situation particulière, ou à tout moment s'il s'agit de prospection.

Comment ces droits s'appliquent-ils à votre recherche ?

En tant que responsable du traitement des données, il vous incombe de faciliter et de permettre l'exercice des droits des personnes concernées. En effet, c'est vers vous que ces personnes se tourneront pour faire valoir leurs droits. Dans le cadre de la recherche, **les demandes les plus fréquentes concernent généralement le droit d'accès, le droit de rectification et le droit à l'effacement**.
Par exemple, un participant à votre étude pourrait demander à consulter les données personnelles que vous avez collectées à son sujet afin de vérifier leur exactitude et leur exhaustivité. S'il identifie une erreur ou souhaite modifier une information fournie, il peut solliciter la rectification de ces données. De plus, si ce participant décide de retirer son consentement à la participation à l'étude, il peut également demander la suppression de ses données personnelles.

Comment traiter une demande d'exercice de droit ?

1) Lorsque vous recevez une demande d'exercice des droits, accusez réception de la demande de manière rapide et professionnelle. Informez l'utilisateur que sa demande a bien été reçue et qu'elle est en cours de traitement.

2) Vérifiez l'identité de l'utilisateur, surtout si la demande concerne des informations sensibles ou la suppression de données. Cela peut nécessiter la confirmation de certaines informations ou documents (par exemple une copie de la pièce d'identité que vous supprimerez après avoir vérifié).

3) Si tout est en règle et que vous avez compris précisément ce que l'utilisateur demande (accès, rectification, suppression, etc.), vous avez un délai d'un mois maximum à partir de la réception de la demande pour la traiter (éventuellement prolongeable de deux mois en cas de complexité). Si tel est le cas, informez l'utilisateur de la prolongation possible et des raisons de ce délai supplémentaire.
Dans le cas contraire, si le périmètre est trop large ou peu clair, vous pouvez demander davantage de précisions à la personne quant à son souhait.

4) Après avoir traité la demande, communiquez la réponse à l'utilisateur de manière claire et détaillée. Par exemple : fournissez les données demandées ou une confirmation que les données ont bien été supprimées.

⚠️ Attention

Si une personne concernée n'est pas satisfaite de la réponse que vous lui apportez, elle a le droit de se tourner vers la CNIL (Commission Nationale de l'Informatique et des Libertés) pour déposer une plainte. En cas de non-conformité au RGPD, votre responsabilité en tant que chercheur pourrait être engagée, entraînant des conséquences juridiques et financières pour vous, vos travaux et pour l'université. Assurez-vous de traiter chaque demande avec le plus grand soin et en respectant les délais impartis. En cas de doutes, vous pouvez contacter votre DPO à l'adresse suivante : dpo@univ-paris1.fr

✅ Bonnes pratiques

Il est important que vous conserviez précieusement les demandes d'exercices de droit reçues et les réponses que vous y avez apportées. Cela servira de preuve en cas de contrôle ou de contestation concernant la gestion des données dans le cadre de votre recherche.

Existe-t-il des limites à l'exercice des droits dans le cadre des travaux de recherche ?

Oui, des limites existent. L'article 89(1) du RGPD prévoit certaines **exceptions**, particulièrement lorsque satisfaire une demande **pourrait entraver gravement la réalisation des objectifs de votre recherche scientifique**. En tant que chercheur, vous pouvez être confronté à des situations où le respect des droits des personnes concernées pourrait compromettre l'intégrité ou les résultats de votre étude car elle ne serait alors plus représentative de la population enquêtée.

Par exemple, imaginez qu'un participant souhaite modifier ou supprimer ses réponses à une enquête ou une interview un an après leur collecte. Si ces données ont déjà été intégrées dans une analyse approfondie, accéder à cette demande pourrait fausser les résultats de votre étude et affecter les conclusions obtenues. De même, si une demande de retrait est faite après la publication des résultats de la recherche, cela pourrait également compromettre la validité de vos conclusions. Dans ces cas, vous pouvez invoquer ces exceptions pour expliquer que satisfaire la demande risque de rendre impossible ou compromettre grandement la réalisation des objectifs et à la validité de la recherche. Toutefois, ces dérogations ne s'appliquent que si des mesures appropriées pour protéger les droits et libertés des personnes concernées ont été mise en place (cf. fiche pratique 11).

⚠️ Attention

Les limitations à l'exercice des droits doivent rester des exceptions et non des règles courantes. Évitez de vous abriter systématiquement derrière ces exceptions, car cela pourrait entraîner des complications. Soyez proactif et transparent : par exemple, informez clairement les personnes concernées du délai pendant lequel elles peuvent soumettre une demande d'exercice de droit. Précisez à partir de quel moment il devient impossible de répondre favorablement en raison de l'avancement des travaux.

🛠️ Pour aller plus loin

- Page CNIL « Comment répondre à une demande de droit d'accès ?» : LIEN
- Schéma « Comment traiter une demande de droit d'accès ? » : LIEN

🎯 Récapitulatif

À la fin de cette fiche, afin de garantir la conformité avec le RGPD, vous devez être capable de reconnaître et de traiter une demande d'exercice de droit formulée par une personne concernée.

Bien que cette fiche ne requière pas d'informations à inscrire dans le registre des traitements, elle est essentielle pour comprendre et préparer la fiche suivante, qui, elle, nécessitera des informations à compléter.

Fiche 8 : Modalités d'information auprès des personnes concernés

Dans la fiche précédente, nous avons vu comment reconnaître et traiter les demandes d'exercice de droits formulées par les personnes concernées. À présent, vous allez découvrir qu'il est tout aussi crucial de **fournir aux participants des informations claires et complètes sur le traitement de leurs données**.

Dans cette fiche, qui complète directement la précédente, nous explorerons en détail les modalités d'information que vous devez mettre en œuvre. Vous apprendrez comment garantir que les personnes concernées sont bien informées de leurs droits et des conditions de traitement de leurs données personnelles.

Pourquoi informer les personnes concernées ?

Les articles 12 à 15 du RGPD soulignent l'importance cruciale de la transparence dans le traitement des données personnelles. En fournissant des informations claires et complètes, les personnes concernées comprennent comment leurs données seront utilisées et peuvent exercer leurs droits en toute connaissance de cause. Une communication transparente renforce également la confiance des participants dans la gestion de leurs données.

⚠️ Attention

L'information offerte aux participants pour leur transmettre les résultats de la recherche à laquelle ils ont contribué ne constitue pas la mention d'information exigée par le RGPD. Bien qu'il s'agisse d'une bonne pratique adoptée par certaines équipes de recherche, cette démarche ne relève pas d'une obligation légale en matière de protection des données.

Quelles informations dois-je obligatoirement fournir ?

Le RGPD précise les informations **obligatoires** à communiquer aux personnes concernées, en incluant des éléments essentiels abordés dans les fiches précédentes :
- L'identité et les coordonnées du responsable du traitement des données (fiche 1)
- Les finalités du traitement (fiche 2)
- La base légale du traitement (fiche 3)
- Les destinataires ou catégories de destinataires des données (fiche 6)
- Les droits des personnes concernées incluant les coordonnées du délégué à la protection des données du projet et le droit de déposer une réclamation auprès de la CNIL (fiche 7)
- La durée de conservation des données (fiche 10)

Cela représente tous les points pour lesquels vous pourriez devoir fournir une preuve de communication. Cela ne signifie pas que vous devez limiter vos échanges avec les participants à ces seuls aspects ; bien au contraire, cela indique simplement que seuls ces éléments seront contrôlés dans le cadre du RGPD.

✅ **Bonnes pratiques**

De plus, lorsque certaines informations sont facultatives, il est recommandé de le préciser directement sur le support de collecte, par exemple en utilisant des astérisques pour distinguer les données obligatoires des données optionnelles. N'oubliez pas d'indiquer les éventuelles conséquences en cas de non-fourniture des données obligatoires.

Quand dois-je informer les personnes ?

La réponse à cette question dépendra de la méthode que vous utilisez pour collecter les données (cf. fiche 5) :

- En cas de collecte directe : il est recommandé de fournir ces informations dans une notice d'information à remettre **avant** ou, au minimum, **au moment de la collecte des données**. Cela permet aux participants de prendre connaissance des conditions du traitement et de bien comprendre les modalités avant de consentir à participer à la recherche.

- En cas de collecte indirecte de données (par exemple, réutilisation de données collectées par des tiers, ou collecte via une API d'une plateforme) : il est impératif d'informer les personnes concernées dans les plus brefs délais et, en tout état de cause, dans un délai d'un mois maximum. Dans le cas où ce délai ne serait pas possible, il est envisageable de communiquer :
  - Soit lors de la première prise de contact avec la personne concernée si cette dernière est contactée directement pour participer à la recherche.
  - Soit, si les données doivent être partagées avec un autre destinataire, au moment de cette transmission.

🔍 **FOCUS : Modalités d'information en cas de réutilisation de données**

Il est crucial de noter que **la collecte indirecte de données ne vous exonère pas de l'obligation d'informer les personnes concernées du traitement de leurs données**, en particulier si ce traitement diffère substantiellement de celui auquel elles avaient initialement consenti, ou si de nouveaux éléments viennent modifier la situation (comme l'ajout d'une nouvelle finalité, de nouveaux destinataires, etc.).
Par exemple : Lorsque des données collectées initialement pour un autre objectif (par exemple, par une institution publique pour sa mission, puis mises en open data) sont réutilisées par un chercheur, ce dernier doit informer de nouveau les personnes concernées.

Les seules exceptions à cette obligation d'information sont les suivantes :
- Lorsque la personne concernée a déjà été informée : Si les données sont collectées indirectement mais que les personnes concernées avaient déjà été informées des modalités de traitement, il n'est pas nécessaire de les informer à nouveau. Par exemple, si des données ont été collectées pour un suivi de cohorte à une année donnée (n) et que le chercheur les utilise l'année suivante (n+1) dans le cadre d'une comparaison, et que les personnes avaient été prévenues de la durée du suivi, il n'y a pas de nouvelle obligation d'information.
- Si fournir ces informations est impossible ou nécessiterait des efforts disproportionnés.
- Lorsque l'information individuelle des personnes est susceptible d'empêcher ou de compromettre gravement la réalisation des objectifs du traitement.

Comment fournir ces informations ?

Il n'existe pas de réponse unique à cette question. L'essentiel est de faciliter l'exercice des droits des personnes concernées, ce qui passe par une communication efficace, quel que soit le support ou la méthode utilisée. Pour vous aider dans cette tâche, un modèle minimal de mention d'information inspiré de celui de la CNIL est mis à votre disposition en ANNEXE 2. Il vous suffit de le compléter en l'adaptant à votre traitement.

Si vous disposez déjà d'un modèle ou document d'information plus complet et détaillé (présentant, par exemple, votre équipe, le contexte et les objectifs de vos travaux, l'importance de la participation des personnes, etc.), surtout ne le jetez pas ! Assurez-vous simplement qu'il inclut toutes les informations obligatoires mentionnées ci-dessus. Le cas échéant, complétez-le au besoin en vous aider du modèle en annexe, afin de pouvoir continuer à l'utiliser sans souci.

⚠️ Attention

La mention d'information ci-dessous ne constitue en aucun cas un consentement des personnes à participer à votre recherche ni une autorisation à collecter et traiter leurs données personnelles. Elle représente uniquement les informations minimales que vous êtes tenu de fournir aux personnes concernées, afin qu'elles puissent, si nécessaire, donner leur consentement éclairé à la participation et à la collecte de leurs données.

✅ Bonnes pratiques

Autant que possible, la mention d'information doit être adaptée au profil des personnes concernées : adultes, enfants, ou individus sous tutelle, les termes employés doivent être appropriés à chaque catégorie. Pour les enfants et les personnes dites « vulnérables », l'information doit également être communiquée aux parents, tuteurs, détenteurs de l'autorité, proches ou personne de confiance, selon les cas. Si votre recherche s'adresse à un public étranger, pensez à rédiger la mention d'information en anglais ou à fournir une version traduite.

Dans la mesure du possible, **essayez de délivrer l'information directement auprès de la personne concernée**. Lorsque cela est impossible ou si cela demande des efforts disproportionnés, d'autres moyens de diffusion plus généraux peuvent être envisagés : communication par liste de diffusion, affichage sur un panneau ou un site internet etc. N'hésitez pas à rendre l'information **aussi accessible que possible** en diversifiant les supports utilisés. Cette approche garantit que les informations restent facilement accessibles pour tous les participants.

En général, la CNIL recommande de fournir les informations en deux étapes, à travers deux supports différents. Par exemple, si vous partagez votre enquête par email, vous pouvez inclure une brève mention à la fin du premier message de contact, telle que : « *[Le responsable du traitement] traite les données recueillies pour [finalités du traitement]. Pour en savoir plus sur la gestion de vos données personnelles et pour exercer vos droits, veuillez consulter [lieu de consultation de la notice détaillée].* [3]»

[3] Si vous rencontrez des difficultés à compléter les champs entre crochets, référez-vous aux fiches explicatives associées (fiche 1 et fiche 2).

Cette approche est également applicable pour une enquête en ligne : vous pouvez insérer une courte mention sur la page de l'enquête, renvoyant à une notice détaillée sur la gestion des données disponible en ligne.

Comment dois-je remplir la fiche du registre ?

Dans la section « **Formalités** », à la fin, vous trouverez un champ intitulé « **Modalités d'information auprès des usagers concernés** ». C'est ici que vous devrez préciser comment vous avez informé les personnes concernées.

En vous basant sur les informations fournies précédemment, n'hésitez pas à donner le maximum de détails : à quel moment avez-vous effectué cette communication (a-t-elle été faite avant la collecte ou le traitement des données) ? Par quel(s) moyen(s) l'avez-vous partagée ? Si votre recherche inclut des participants étrangers, avez-vous préparé une version en anglais pour garantir une accessibilité optimale ? Détaillez soigneusement les circonstances et la méthode par lesquelles vous avez rempli cette obligation d'information.

Les documents utilisés pour informer les participants doivent être ajoutés en pièce jointe à la fiche du registre des traitements, dans le champ « **Fichier(s) d'information** ». N'hésitez pas à faire des captures d'écran si les documents ne sont pas dans un format facilement exportable.

Enfin, dans le champ « **Coordonnées de la personne auprès de laquelle s'exerce le droit d'accès** », vous n'aurez qu'à copier les informations que vous avez déjà fournies dans votre mention d'information.
Par défaut, nous pouvons afficher notre adresse email si vous n'avez pas d'autre moyen de contact. Cela peut être une solution temporaire, mais assurez-vous que le DPO soit informé et que la fiche du registre soit en cours de complétion. Cela dit, nous vous encourageons fortement à inclure également vos propres coordonnées, car ce sont souvent celles avec lesquelles les personnes concernées tenteront spontanément de vous joindre.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Modalité d'information auprès des usagers concernés**
- **Fichier(s) d'information**
- **Coordonnées de la personne auprès de laquelle s'exerce le droit d'accès**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 9 : Sauvegarde et stockage des données

Aujourd'hui, l'essentiel de la production scientifique est créé, traité, stocké et diffusé sous forme numérique. Ainsi, que vous soyez doctorant ou chercheur, les notions de stockage (supports physiques) et d'hébergement des données (supports en ligne) vous concernent directement. Pour chaque projet de recherche, il est essentiel de se poser la question suivante : Sur quels types de supports vais-je conserver mes données ?
Dans la plupart des cas, une combinaison de ces deux solutions sera utilisée. Cette fiche a pour objectif de vous éclairer sur ces deux concepts et de vous guider vers l'adoption des bonnes pratiques adaptées à vos besoins.

Où stocker et héberger vos données de recherche ?

Il existe de nombreuses façons de gérer vos données pendant le processus de recherche : sauvegardes des données sur des ordinateurs personnels, des disques durs (internes ou externes), des clés USB, des serveurs institutionnels ou le cloud via différents services d'hébergement… **Les solutions sont multiples mais toutes ne se valent pas**.

Privilégiez, dans la mesure du possible, **les plateformes institutionnelles ou les infrastructures disciplinaires.** L'Université Paris 1 met à votre disposition un espace cloud institutionnel SharePoint, accessible via votre ENT.
Si cette capacité ne suffit pas, plusieurs infrastructures de l'ESR proposent des solutions de stockage de données plus développées. Par exemple, Huma-Num[4] est une grande infrastructure de recherche dédiée aux sciences humaines et sociales. Parmi ses services, on trouve ShareDocs[5], un gestionnaire de fichiers permettant de préparer vos données en vue de leur diffusion. Cet espace collaboratif, adapté à un usage multi-laboratoires, propose de nombreuses options de paramétrage pour les droits des dossiers et fichiers. Il offre également une capacité de stockage de 90 Go pour un compte personnel à titre individuel ou 300 Go dans le cadre d'un projet d'équipe. De plus, Huma-Num garantit un stockage sécurisé sur les serveurs du CNRS situés en France, à Villeurbanne. Ces services sont accessibles à toute personne appartenant à l'Enseignement Supérieur et de la Recherche (ESR) ou participant à un projet piloté par des membres de l'ESR, sur simple demande.

Il est déconseillé de stocker les données sur des ordinateurs portables, des disques durs externes ou des supports de stockage tels que des clés USB. Si l'utilisation d'un disque dur est inévitable, optez pour des supports protégés par mot de passe ou des disques sécurisés « RAID » en « direct access storage » (DAS).

Quelles sont les recommandations à garder en tête ?

La gestion des données, en particulier en ce qui concerne leur stockage et leur hébergement, est un élément clé du processus de mise en conformité. **L'objectif n'est pas de privilégier des solutions pratiques pour votre usage quotidien, mais de penser les premières mesures de sécurité pour les qui vous sont confiées**.

[4] https://s3.fr-par.scw.cloud/rdg-portal/documents/GT3_Fichespratiques_HUMANUM.pdf
[5] https://sharedocs.huma-num.fr/wl/?id=rjKGsfd9fkgHvvsbFp8hiCsOGLRYBgAQ

- **Respect de la règle du 3-2-1** : La règle du 3-2-1 est une bonne pratique en gestion de la sauvegarde des données. Elle consiste à conserver 3 copies des données (l'original + 2 sauvegardes) sur 2 supports ou technologies différents (par exemple, un disque dur chiffré et un stockage cloud institutionnel), dont 1 copie doit être stockée hors site (dans un endroit séparé pour se protéger contre les incidents locaux : incendie, vol, inondation, etc.). Cette approche garantit que les données restent accessibles même en cas de panne ou de sinistre.

✅ Bonne pratique

Veillez à bien répertorier tous les supports utilisés, actuels ou passés, pour le stockage et l'hébergement de vos données de recherche (en somme, décrire les flux de donnée). Cela vous sera particulièrement utile au moment de la suppression des données, en vous permettant de nettoyer de manière exhaustive l'ensemble des supports sans risque d'oubli.

- **Adaptez le support à la sensibilité de vos données** : Tous les supports ne se valent pas en matière de sécurité. Par exemple, si vous manipulez des données de santé (généralement les plus sensibles), vous ne pouvez pas les stocker n'importe où : vous devez impérativement sélectionner un espace certifié « Hébergement des données de santé » (dit HDS).

De la même manière, le stockage de données sur des services de cloud grand public (comme Google Drive, Dropbox, etc.) est fortement déconseillé. Bien que ces services soient très pratiques pour un usage personnel, ils ne garantissent pas toujours une protection suffisante des données personnelles, surtout lorsqu'il s'agit de données de recherche sensibles. Vous pouvez utiliser ces services pour vos propres données personnelles si vous le souhaitez, mais ne les utilisez pas pour des travaux de recherche contenant des données personnelles appartenant à d'autres personnes.
Si vous ne pouvez pas utiliser un entrepôt de confiance, essayez d'optez pour des plateformes d'hébergement certifiées (mais payantes), comme SecNumCloud, qui offrent un niveau de sécurité élevé pour vos données de recherche sensibles.

⚠️ Attention

Si vous travaillez dans un laboratoire ou une unité associée au CNRS, il est interdit de stocker des données sensibles ou liées à la souveraineté de la France sur des infrastructures cloud « grand public », en raison des lois extraterritoriales qui permettent à des gouvernements étrangers d'accéder à vos données.

Je vous recommande de consulter le correspondant sécurité CNRS de votre unité pour connaître les consignes spécifiques à suivre dans votre cas. Si nécessaire, demandez-lui de vous indiquer les options de stockage sécurisé qu'il peut vous proposer.

- **Considérez les besoins spécifiques de votre projet** : Prenez en compte les besoins spécifiques de votre projet lors du choix d'une solution de stockage ou d'hébergement. Soyez particulièrement attentif à la nécessité de collaboration et à la fréquence des échanges et partages de données au sein de votre équipe. Si vous choisissez de ne pas utiliser des solutions d'hébergement et de vous limiter à des techniques de stockage, sachez que vous rencontrerez rapidement des difficultés lorsque vous souhaiterez partager vos données pour collaborer. En effet, pour des raisons de sécurité, il est crucial de limiter autant que possible les échanges de

données par email sans mesures de protection supplémentaires, afin de prévenir les risques d'erreurs humaines, de fuites ou d'accès non autorisés.

- **Faites attention au pays d'hébergement de vos données** : Si vous choisissez une solution d'hébergement en ligne, veillez à vérifier l'emplacement et le pays où se trouvent les serveurs de cette solution. Si possible, privilégiez les espaces qui utilisent des serveurs situés en Europe, avec bien entendu une préférence pour ceux hébergés en France.

🔍 FOCUS : Pourquoi est-il important de se préoccuper du lieu d'hébergement ?

Le RGPD impose des règles strictes concernant le transfert de données personnelles en dehors de l'Union européenne. Héberger des données dans des pays extérieurs à l'UE, qui ne garantissent pas un niveau de protection adéquat, peut être illégal ou nécessiter des garanties supplémentaires.

En effet, les pays hors de l'UE n'ont pas toujours les mêmes normes de sécurité que celles requises par les réglementations européennes. Stocker des données sensibles dans des régions avec des standards de sécurité moins stricts peut exposer vos données à des risques accrus de cyberattaques, de piratage ou de vols de données.

Par exemple, si vos données sont hébergées aux États-Unis, elles peuvent être soumises à des lois comme le Cloud Act, qui permet aux autorités américaines d'accéder à certaines données, même si elles concernent des citoyens européens.

Que dois-je indiquer dans la fiche du registre ?

Dans la section « **Sécurité des données (technique)** », vous trouverez un champ intitulé « **Hébergement des données** », où vous devrez sélectionner la solution de stockage et/ou d'hébergement privilégiée à l'aide d'une liste déroulante.

Comme vous ne pouvez indiquer qu'une seule option, je vous recommande de sélectionner la solution principale dans le menu déroulant. Ensuite, utilisez le champ libre « **Autres précisez** » situé juste en dessous pour décrire en détail la ou les solutions choisies et les raisons de votre choix.

Enfin, il reste un point essentiel en lien avec les supports de stockage et d'hébergement : la liste des applications logicielles utilisées. Vous trouverez le champ « **Application(s) logiciel(s) utilisée(s)** » dans la section « **Formalités** ». À ce stade de votre démarche de conformité, vous devriez avoir une vision claire des outils que vous utiliserez pour traiter les données personnelles et pouvoir ainsi remplir ce champ. Il s'agit simplement de répertorier toutes les applications et logiciels prévus pour vos travaux (ce champ est évolutif et peut être mis à jour au fil de vos recherches pour ajouter de nouveaux outils ou retirer ceux qui s'avèrent inutiles). Tâchez d'être aussi exhaustif que possible.

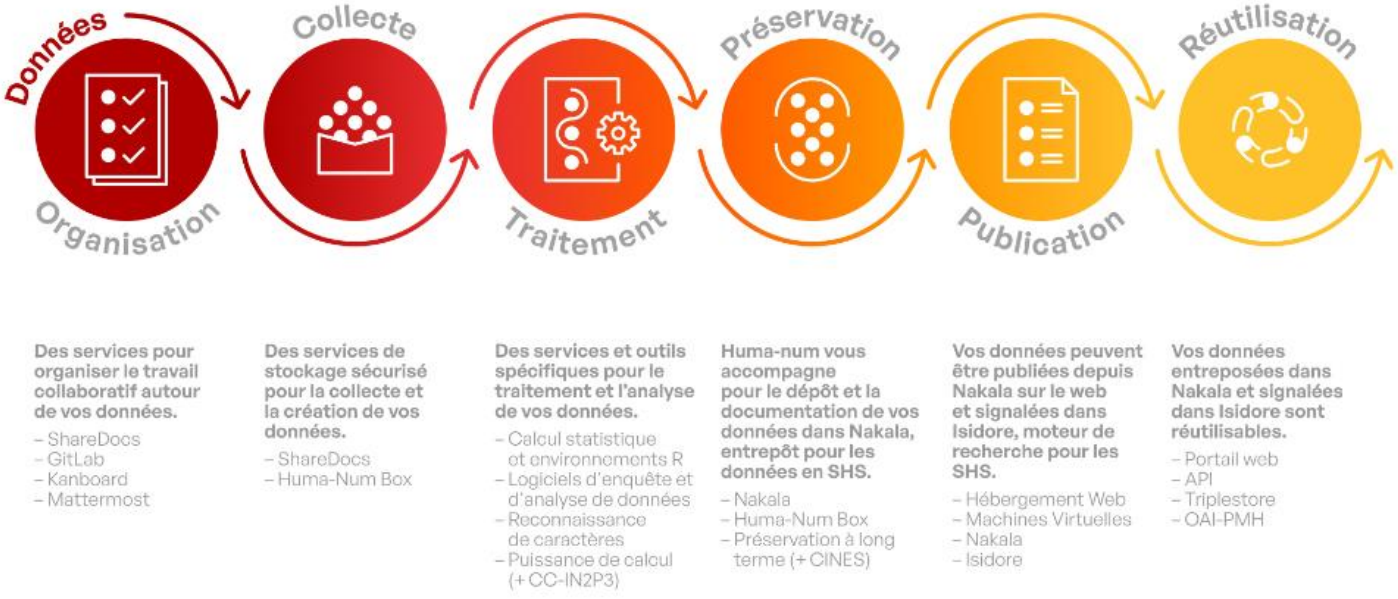
📌 Exemples

- Outils M365 collaboratifs : Word, Excel, PowerPoint…
- Logiciel de captation des entretiens
- Logiciel de QDA pour l'exploitation des données en précisant le besoin
- Logiciel d'enquête et sondage
- Carnet hypothèse
- Outils LLM d'IA

Cette liste vise à vous aider à cerner vos besoins spécifiques. L'objectif sera de comprendre le circuit des données, ce qui facilitera l'identification des risques et des mesures de sécurité à appliquer dans la fiche suivante.

✅ Bonne pratique

Si vous n'êtes pas certain des outils à utiliser ou si votre budget ne permet pas d'investir dans de nombreuses licences payantes, sachez que l'infrastructure Huma-Num, mentionnée précédemment, propose une large gamme d'outils pour vous accompagner dans le traitement des données tout au long de leur cycle de vie (voir capture ci-dessous).



🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :

- **Application(s) logiciel(s) utilisée(s)**
- **Hébergement des données**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 10 : Durée de conservation et archivage

Après avoir exploré les options de stockage et sauvegarde dans la fiche précédente, il est maintenant essentiel de se concentrer sur la **durée de conservation de vos données**.
La durée pendant laquelle vous conservez les données est un aspect clé pour garantir la conformité au RGPD. En effet, une conservation excessive ou insuffisante peut entraîner des problèmes de conformité ainsi que des risques pour la sécurité des données.

Comprendre le cycle de vie des données en matière de conservation

La conservation des données prévoit un cycle en trois temps, selon l'avancement de votre projet :

- **Phase 1 - la base active** : Elle correspond à l'utilisation courante des données, soit le temps de la recherche. À ce stade, les données sont dites « chaudes », car elles sont fréquemment modifiées et accédées. Elles doivent donc être facilement accessibles et régulièrement mises à jour, tout en veillant à appliquer des mesures de sécurité adaptées.

- **Phase 2 - l'archivage intermédiaire** : Les données à caractère personnel peuvent, dans certaines conditions, être conservées à l'issue du traitement des données mais avec un accès restreint. En effet, une fois le projet terminé, les données sont conservées pour des besoins de recherche, statistiques, historique ou archivage. L'objectif ici est une conservation à moyen ou long terme, pour permettre une réutilisation ou une valorisation ultérieure. Par exemple, au CNRS, la durée d'archivage intermédiaire est souvent de deux années après la dernière publication des résultats de la recherche.

- **Phase 3 – l'archivage définitif** : L'archivage pérenne vise à garantir la conservation, l'accès et l'intelligibilité des données sur le long terme (généralement plus de 30 ans). Seules les données présentant une valeur scientifique importante et reconnue par la communauté scientifique sont concernées par cette phase. Il peut s'agir de données uniques, non reproductibles ou coûteuses, souvent issues de projets d'intérêt public. L'archivage définitif ne peut pas être réalisé dans le laboratoire. Il est effectué avec les services d'Archives départementales ou nationales en lien avec les établissements de rattachement du laboratoire.
En France, c'est le CINES qui a été mandaté comme opérateur national pour l'archivage des données de l'enseignement sup et de la recherche.

✅ Bonne pratique

Une fois votre projet terminé, pour garantir que vos données restent accessibles et bien conservées sur le long terme, il est souhaitable de les déposer dans un entrepôt de données. Cet espace permet de les rendre accessibles facilement et de permettre leur réutilisation par des chercheurs du même domaine ou d'un autre domaine, selon les principes FAIR sur le court et le moyen terme, mais aussi de les conserver de façon durable et sécurisée.

Pour aller plus loin : https://science-ouverte.pantheonsorbonne.fr/ouvrir-science/gerer-ses-donnees

Que dit le RGPD en matière de durée de conservation ?

Contrairement à une idée reçue, **le RGPD ne fixe pas de durée de conservation spécifique pour les traitements de données**. En raison de la diversité des situations, il serait impossible de déterminer une règle unique pour tous les cas.

Cependant, le RGPD établit un principe fondamental : les données personnelles doivent être conservées **uniquement pendant la période nécessaire à la réalisation des objectifs pour lesquels elles ont été collectées** (article 5(1)(e)). En règle générale, il est interdit de conserver des données « à vie ». Cette obligation concerne aussi bien les fichiers informatiques et les fichiers.
Par ailleurs, pour rappel, les durées de conservation des données doivent être porter à la connaissance des personnes concernées par le biais de mentions d'information (cf. fiche pratique 8).

🔍 FOCUS : Conservation prolongée autorisée dans le cadre des données de recherche

Les projets de recherche nécessitent souvent une conservation prolongée des données, incluant leur ouverture au public et leur réutilisation. Bien que ces pratiques impliquent des durées de conservation longues, voire indéterminées, elles restent permises sous certaines conditions.

En effet, bien que le RGPD insiste sur le principe de limitation de la durée de conservation des données personnelles, il reconnaît l'importance des traitements à des fins de recherche scientifique, historique ou archivistique dans l'intérêt public. Il prévoit donc des exceptions spécifiques pour ces traitements.

Ainsi, pour concilier la limitation de la conservation avec la nécessité de stocker des données à long terme dans des projets de recherche, les articles 5(1)(e) et 89(1) permettent la conservation des données personnelles plus longtemps lorsqu'elles sont utilisées exclusivement à des fins archivistiques, scientifiques ou statistiques.
Toutefois, cette conservation prolongée doit s'accompagner de mesures techniques et organisationnelles appropriées afin de protéger les droits et libertés des personnes concernées : anonymisation, pseudonymisation, obtention du consentement et mise en place de mesures de sécurité adaptées.

Comment déterminer la durée de conservation de mes données ?

Il est nécessaire de déterminer une durée de conservation des données en amont de la mise en œuvre du traitement à finalité de recherche. Avant toute chose, revenez à vos finalités de traitement (cf. fiche pratique 2) et réfléchissez à l'objectif poursuivi par la collecte et le traitement des données. Ensuite, posez-vous les bonnes questions :

- Pendant combien de temps les données seront-elles nécessaires pour atteindre l'objectif de la recherche ?
- Mon étude impose-t-elle des durées de conservation spécifiques ?
- Existe-t-il des obligations réglementaires ou des politiques institutionnelles concernant la conservation des données ?
- Une fois ma recherche et l'analyse des données achevées, ai-je toujours besoin de conserver l'intégralité de mes bases de données ?

En fonction de ces questions, la durée de conservation peut être déterminée selon deux modalités :

- De manière précise, à partir d'un **événement certain ou d'une date fixée**. Par exemple : 3 ans à compter de la fin de la collecte des données, pour permettre l'analyse et la production des résultats de la recherche ; ou encore 3 ans à compter de la date de la dernière publication scientifique.
- Selon la survenance d'un **événement spécifique et certain**, lorsque la durée exacte ne peut être définie à l'avance. Dans ce cas, **précisez les critères qui orienteront la décision d'effacement**. Par exemple : jusqu'au lancement d'une nouvelle enquête si une deuxième vague est prévue, 2 ans après la publication d'une recherche, ou 6 mois après la fin d'un colloque

Toutes les catégories de données que vous traitez ne sont pas nécessairement soumises aux mêmes durées de conservation. Pensez à **adapter ces durées en fonction du type de données collectées, leur utilité et leur sensibilité**. Vous disposez d'une certaine flexibilité pour définir ces durées, tant qu'elles sont justifiées par les besoins spécifiques de votre projet.
N'oubliez pas non plus de préciser la fréquence à laquelle vos bases de données seront mises à jour, si cela est pertinent, ainsi que la personne responsable de cette mise à jour (par exemple : au fil de l'eau selon les réponses reçues ou à des dates précises).

Pour vous guider dans votre réflexion, je vous recommande de consulter le « **Référentiel de gestion des archives de la recherche** » de l'Association des archivistes français. À partir de la page 8, vous trouverez des recommandations et indications utiles concernant les durées de conservation et le sort final des données, selon différents types de données scientifiques de recherche. Vous pouvez accéder au document ici : https://doranum.fr/wp-content/uploads/Referentiel_2.pdf

📌 **Exemples**

Voici des exemples concrets de réponses fournies par d'autres chercheurs dans le cadre de leurs projets. Ils illustrent leurs réflexions, mais ne sont pas destinés à être copiés tels quels : **la justification des durées de conservation doit être adaptée aux besoins spécifiques de votre projet**. N'hésitez pas à appliquer cette même démarche à l'ensemble des données personnelles que vous traitez.

- Données d'identification : Ces données seront conservées environ 2/3 ans après la fin du projet de recherche, justifiées par la possibilité de solliciter les participants pour des articles, publications ou communications ultérieures.

- Données de contact : Il sera nécessaire de conserver uniquement les moyens de contact (nom et prénom inclus) pendant 5 ans après le projet, afin de faciliter une étude comparative ou longitudinale avec les mêmes participants à ce moment-là.

- Enregistrements audios/vidéos : Un chercheur a prévu de les supprimer immédiatement après leur retranscription, estimant qu'ils ne sont plus nécessaires. À l'inverse, un autre a justifié une conservation prolongée jusqu'à la fin de la recherche, afin de pouvoir vérifier les transcriptions en tenant compte des intonations, pauses et nuances, lors d'une relecture orale ultérieure des témoignages par des intervenants.

- Demandes de contact : Les données issues de contacts par mail ou formulaire seront supprimées une fois la demande traitée, sauf si une conservation plus longue se justifie par des besoins spécifiques.

✅ Bonnes pratiques de conservation des données de recherche

- Les données identifiantes des personnes qui n'ont pas consenti à la recherche ou qui ont retiré leur consentement doivent être supprimées dès que possible, à condition que cela ne compromette pas le déroulement des recherches.

- Les données directement identifiantes (nom, prénom, adresse, numéro de téléphone, plaque d'immatriculation, etc.) des participants contribuant à la constitution de l'entrepôt doivent être supprimées une fois que les informations (comme les retranscriptions d'entretiens ou les vidéos) ont été intégrées dans la base de données.

- Dans le cadre de financements de recherche ou de valorisation des résultats, les données personnelles peuvent être conservées au moins pendant la durée du projet, avec une période supplémentaire de deux ans par exemple pour permettre la publication, la vérification, la valorisation ou une éventuelle reprise des études, lorsque l'anonymisation n'est pas réalisable.
À titre indicatif, la CNIL considère qu'une durée de conservation des données personnelles allant jusqu'à cinq ans après la dernière publication scientifique peut être justifiée si nécessaire [6].

- Au-delà de la période conservation définie, les données doivent êtres anonymisées, supprimées ou archivées.

🔍 FOCUS : Dois-je conserver l'ensemble des données produites ?

Dans le cadre de vos recherches, vous produisez ou collectez un grand volume de données. Toutefois, il est nécessaire d'opérer une sélection progressive. Ainsi, une distinction doit être faite entre les données initialement produites, celles effectivement traitées, celles finalement retenues, et en dernier lieu, les données qui seront publiées. À chaque étape de ce processus, le volume de données se réduit.

Vous devez trouver un juste équilibre entre la conservation et la suppression des données. Cela implique de sélectionner les données essentielles à conserver et d'éliminer celles qui n'ont plus d'utilité administrative, scientifique, statistique ou historique.

Cependant, bien qu'il ne soit pas nécessaire de conserver toutes les données produites au cours de vos recherches, ne conserver que les données publiées peut parfois être insuffisant. Il est recommandé de conserver les données qui permettent non seulement de comprendre et d'évaluer le projet, mais aussi d'en assurer la reproductibilité, voire d'approfondir les recherches à l'avenir.

[6] Dans un avis du 27 février 2020 sur un projet d'enquête de l'INED concernant les immigrants chinois à Paris et en région parisienne et visant à mettre en évidence les aspects cruciaux d'assimilation des immigrants dans le contexte français.

Comment garantir la vérification des résultats de recherche tout en respectant le RGPD ?

Bien que l'article 89 du RGPD permette d'allonger les durées de conservation des données à des fins de recherche, il impose également qu'elles ne soient pas conservées indéfiniment. Elles doivent donc faire l'objet, à terme, soit d'une suppression, soit d'un archivage. Or, la recherche scientifique impose une exigence inverse : la Charte nationale de déontologie des métiers de la recherche stipule que les données brutes et les analyses doivent être conservées afin de garantir la possibilité de vérification des résultats.

L'anonymisation pourrait sembler être une solution adaptée. Cependant, elle empêche de remonter jusqu'aux personnes concernées, rendant ainsi impossible la vérification et l'authentification des résultats (comment prouver qu'il ne s'agit pas d'une fabrication de données ?).
À l'inverse, conserver indéfiniment l'ensemble des questionnaires, fichiers Excel, enregistrements audios et vidéos contenant des données personnelles ne serait pas conforme aux principes du RGPD.

Si le RGPD impose une durée de conservation pertinente et proportionnée aux finalités du traitement, en réalité, la conservation des données personnelles à des fins de vérification des résultats peut parfaitement être justifiée au regard de la finalité initiale de la recherche. De plus, cette vérification nécessite rarement des données directement identifiantes : des mesures de minimisation sont donc appliquées, comme la pseudonymisation et la sécurisation des jeux de données soumis à contrôle.

La vérification des résultats ne doit pas être perçue comme une simple prolongation de la durée de conservation des données, mais comme une étape fondamentale du processus scientifique. En effet, la validation par les pairs fait partie intégrante de la recherche et ne s'arrête pas à la publication des résultats. **La mise en place d'un délai post-publication pour la vérification et la remise en cause des résultats dans un cadre raisonnable devrait donc être systématiquement prévue.**

Que dois-je faire une fois la durée de conservation atteinte ?

Trois options s'offrent à vous :
Archivage : Pour les données qui doivent être conservées au-delà de la période active du projet, en raison d'obligations légales ou parce qu'elles ne peuvent pas être supprimées, vous pouvez opter pour l'archivage définitif dans un service public d'archives. Cela limite l'accès aux données tout en assurant leur conservation de manière pérenne et sécurisée.

Anonymisation : L'anonymisation est une alternative permettant de retirer toutes les informations personnelles tout en conservant les réponses, résultats et analyses. Une fois anonymisées, les données ne sont plus soumises au RGPD et peuvent être conservées indéfiniment. Attention, l'anonymisation doit être irréversible, c'est-à-dire qu'il ne doit plus être possible d'identifier la personne concernée, même par recoupement de plusieurs bases de données.

Suppression : La suppression définitive des données est la solution la plus simple et rapide. Cependant, veillez à bien effacer les données de tous les supports sur lesquels elles se trouvent : boîtes mails, pièces jointes, fichiers/dossiers, disques durs, clés USB, cloud, etc.

Une nouvelle fois, en cas de doute, n'hésitez pas à consulter les recommandations du « Référentiel de gestion des archives de la recherche ».

Que dois-je indiquer dans la fiche du registre ?

Vers la fin de la page du registre, vous trouverez une section complète intitulée « **Durée de conservation** », qui comporte trois champs.

Commencez par le premier champ « **Durée de conservation** », où vous pourrez indiquer toutes les durées que vous avez définies en fonction des objectifs de traitement pour chaque type de donnée. Par exemple, si vous avez identifié trois durées de conservation distinctes, vous devrez ajouter trois champs supplémentaires. Une fois qu'un champ est ajouté, cinq sous-champs apparaîtront pour détailler cet ajout :
- « **Type de données** » : Indiquez ici les données concernées par cette durée de conservation.
- « **Conservation en base active** » : Précisez ici la durée pendant laquelle les données collectées seront utilisées, analysées et traitées quotidiennement dans le cadre de votre projet. En toute logique, cette durée doit correspondre à la durée de conservation pour laquelle vous avez créé ce champ.
- « **Justification** » : Fournissez une justification pour le choix de cette durée. Celle-ci pourra varier en fonction des différentes données, même si elles partagent la même durée de conservation.
- « **Conservation en base intermédiaire** » et « **Justification** » : Ce champ concerne l'archivage pour les chercheurs concernés. Indiquez à partir de quand les données ne seront plus facilement accessibles, consultables ou modifiables (transfert en archive), ainsi que la durée légale de conservation, en la justifiant dans le champ qui suit. Pour la plupart d'entre vous, il est peu probable que des données personnelles soient archivées, car elles auront été complètement anonymisées. Dans ce cas, vous pouvez simplement indiquer « N/A ».

Comme vous l'avez sans doute compris, ce processus devra être répété pour chaque durée de conservation identifiée.

Une fois que vous avez terminé, choisissez dans le champ « **Destruction ou reversement aux archives** » l'option qui s'applique à votre situation dans la liste déroulante, puis justifiez et explicitez votre choix dans le champ « **Commentaire** » qui suit.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Durée de conservation**
- **Destruction ou reversement aux archives**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 11 : Sécurité des données

Dans les fiches précédentes, nous avons souvent évoqué l'importance de mettre en place des « mesures techniques et organisationnelles appropriées » pour protéger les données traitées.

Sécuriser les données de la recherche : une obligation ?

La sécurité des données de recherche est une **exigence** incontournable du RGPD, et elle est spécifiquement encadrée par l'article 32, qui énumère plusieurs mesures techniques et organisationnelles pour protéger les données. Bien que cette liste ne soit pas exhaustive, elle souligne que les mesures doivent être **adaptées en fonction des caractéristiques du traitement** : type de données sensibles, risques particuliers, présence de personnes vulnérables, etc.

En plus de cet article général, le RGPD renforce cette obligation pour les acteurs de la recherche à travers l'article 89-1, rappelant que le chercheur doit garantir la sécurité des données par des mesures techniques et organisationnelles appropriées. Cette obligation est même une condition essentielle pour bénéficier des libertés spécifiques prévues pour la recherche, comme le traitement de données sensibles ou l'allongement des durées de conservation.
En somme, vous ne pouvez pas faire l'impasse sur cette étape : assurer la sécurité des données est un élément central de votre conformité !

Que signifie « sécuriser les données » ? Contre quels risques se prémunir ?

La mise en place de mesures de sécurité vise à protéger contre trois principaux risques liés à l'utilisation et au traitement des données personnelles :
- Risque de **perte de disponibilité des données** : cela concerne l'incapacité à accéder ou récupérer des données, les rendant ainsi inaccessibles.
- Risque de **perte d'intégrité des données** : cela implique la protection contre toute modification non autorisée des données personnelles.
- Risque de **perte de confidentialité des données** : il s'agit de prévenir tout partage ou accès non autorisé aux données personnelles.

Il n'existe pas de référentiel clé en main rassemblant toutes les exigences de sécurité que vous devez suivre car les bonnes pratiques et mesures de sécurité techniques mises en œuvre doivent se faire en fonction de chaque projet. Ces mesures doivent être **proportionnées en fonction de la sensibilité des données traitées** : plus les données sont sensibles, plus la sécurité et la confidentialité doit être importante. Il ne s'agit pas d'appliquer toutes les mesures listées à chaque actif, mais de sélectionner celles qui sont les plus pertinentes pour votre projet de recherche.

La suite de ce document va présenter les deux grandes catégories de mesures de sécurité à mettre en œuvre dans le cadre d'un projet de recherche pour prévenir ces risques : les mesures « **techniques** » et les mesures « **logiques** » ou organisationnelles. Ces deux types de mesures sont complémentaires et doivent être soigneusement réfléchis et combinés.

Quelles mesures de sécurité technique mettre en œuvre ?

Les mesures techniques désignent tous les **dispositifs et solutions informatiques** déployés pour protéger les données personnelles. Cela implique de recenser et d'identifier tous les supports numériques sur lesquels les données personnelles circulent car ces actifs numériques représentent des points de vulnérabilité potentielle, chacun nécessitant des mesures spécifiques pour renforcer leur sécurité.
Cette liste n'est pas exhaustive et devra être complétée et ajustée selon les spécificités de votre projet (par exemple, vous pourriez déjà appliquer des mesures plus strictes ou différentes).
Enfin, notez que certaines mesures de sécurité peuvent être déployées de manière polyvalente : ce qui est efficace pour un actif pourrait l'être également pour d'autres types d'actifs.

Bien entendu, il est évident que si le projet de recherche implique plusieurs membres, ces mesures de sécurité doivent s'appliquer à chacun d'eux qui traite ou est amené à traiter des données personnelles.

Selon le guide de la CNIL sur la recherche scientifique (hors santé) [7], les mesures de sécurité technique à mettre en œuvre peuvent être regroupées en quatre catégories : gérer les accès aux données (1), sécuriser les équipements (2), conserver les données (3) et superviser la diffusion des données (4). La plupart des recommandations qui suivent en sont directement inspirées.

1) Gérer les accès aux données

Authentifier les utilisateurs : Il est essentiel de s'assurer que **seuls les utilisateurs autorisés puissent accéder aux données personnelles dont ils ont besoin**.

✅ Bonnes pratiques en matière d'authentification

- Chaque utilisateur doit être doté d'un couple identifiant/mot de passe qui lui est propre. Il est en particulier recommandé de ne pas utiliser de comptes partagés entre plusieurs utilisateurs.
- En fonction de la sensibilité des données conservées, la CNIL estime qu'un mécanisme d'authentification multifacteur, comprenant au moins deux facteurs différents d'authentification, doit être mis en œuvre.

🔍 FOCUS : Gestion sécurisée des mots de passe

- Ne partagez jamais vos mots de passe et veillez à les garder strictement confidentiels.
- Stockez-les de manière sécurisée, en utilisant un gestionnaire de mots de passe ou un fichier chiffré, plutôt que sur un support papier ou dans un endroit facilement accessible. De même, évitez de vous les envoyer par e-mail.
- Protégez l'accès à vos mots de passe enregistrés en activant un mot de passe maître si vous les conservez dans votre navigateur.
- Personnalisez immédiatement les mots de passe par défaut dès la première utilisation.
- Créez des mots de passe uniques et robustes, sans lien direct avec vous (évitez noms, dates de naissance, etc.).
- Ne réutilisez jamais un même mot de passe sur plusieurs services, notamment en évitant d'utiliser vos identifiants institutionnels sur des sites personnels.

[7] https://www.cnil.fr/fr/recherche-scientifique-hors-sante/mesures-de-securite-et-de-confidentialite

💡 Mieux vaut un seul mot de passe solide que des changements trop fréquents, qui peuvent être contre-productifs. Modifiez votre mot de passe uniquement en cas de suspicion de compromission.

Gérer les habilitations : Définir des profils d'habilitation permet de restreindre l'accès des utilisateurs **aux seules données strictement nécessaires en fonction des tâches et domaines de responsabilité de chacun**, afin que seuls ceux qui en ont besoin puissent y accéder.

✅ **Bonnes pratiques en matière d'habilitation**

- Créer et utiliser des comptes individuels pour chaque utilisateur afin de garantir un suivi sécurisé.
- Accorder à chaque utilisateur uniquement les privilèges nécessaires à l'accomplissement de ses tâches, en respectant le principe du moindre privilège.
- Supprimer les comptes des utilisateurs ayant quitté le projet ou changé de mission dès que possible pour maintenir la sécurité et éviter tout accès non autorisé.
- Utiliser un compte avec des privilèges limités pour les tâches quotidiennes et n'élever les privilèges d'administrateur que lorsque cela est strictement nécessaire pour éviter tout risque de mauvaise manipulation ou de sécurité.

Tracer les accès aux données : Selon la nature des recherches, le nombre d'accès et la sensibilité des données, il peut être utile de mettre en place un **système de traçabilité des accès** (grâce à la mise en place précédente d'un mot de passe et identifiant personnel permettant de contrôler les accès) et des **procédures pour gérer les incidents**, notamment en cas de violation de données. Cela permet de réagir rapidement et d'identifier l'origine de l'incident (accès frauduleux, abusif, etc.). Le système de journalisation peut comporter l'enregistrement des activités des utilisateurs comme : identifiant, horaires de connexion et déconnexion, actions effectuées etc. pour suivre l'accès aux données.

2) Sécuriser les équipements

Les risques d'intrusion dans les systèmes informatiques sont importants et **les postes de travail en constituent un des principaux points d'entrée**. Il est donc indispensable de prévenir les accès frauduleux, l'exécution de virus, la prise de contrôle à distance ou le vol d'un équipement.

Protéger son poste de travail : Idéalement, ces équipements sont fournis et administrés par les services informatiques des organismes employant les personnels de recherche, afin que ces derniers puissent se charger pour vous des bonnes pratiques ci-dessous. Si l'utilisation d'un équipement personnel est nécessaire, il est crucial de mettre en place les mesures de sécurité appropriées :

✅ **Bonnes pratiques en matière de poste de travail**

- Authentifier les utilisateurs à l'ouverture de session (cf. partie précédente).
- Mettre à jour régulièrement le système d'exploitation et les logiciels de mon matériel pour corriger les failles de sécurité et prévenir les risques de piratage. Si besoin, activer les mises à jour automatiques.
- Être équipés d'un antivirus régulièrement mis à jour.
- Disposer de pare-feu (firewall).

- Bénéficier d'un disque dur chiffré en cas de perte ou de vol de matériel.

🔍 FOCUS : séparer usage professionnel et personnel

- Je réserve le matériel institutionnel à un usage strictement professionnel et évite d'y stocker ou télécharger des fichiers personnels (photos, vidéos, etc.) pour limiter les risques d'infection.
- Je ne me connecte pas à mes comptes personnels (réseaux sociaux, messagerie privée) sur le matériel de l'institution afin d'éviter les risques de phishing et de confusion entre données personnelles et professionnelles.
- Je ne partage pas mon matériel institutionnel avec des proches pour prévenir toute consultation accidentelle de données sensibles, installation de logiciels non sécurisés ou contamination par des malwares.

Sécuriser l'informatique mobile : La mobilité est souvent une nécessité, vous conduisant à travailler depuis des lieux variés, tels que votre domicile, des espaces de coworking, des laboratoires ou même en déplacement. Les voyages, parfois fréquents, notamment à l'étranger, accentuent cette dynamique. Cependant, ce mode de travail présente des vulnérabilités accrues pour la sécurité de vos équipements : **près de 40 % des vols ou pertes de matériel professionnel surviennent lors de déplacements**, exposant ainsi les données à des risques considérables. Ainsi, si vos activités impliquent des déplacements fréquents pour vous ou vos équipes, il est essentiel d'accorder une attention particulière à la sécurité des appareils et terminaux mobiles.
Par exemple, en janvier 2025, la CNIL polonaise a infligé une amende de 5 700 € suite à la perte d'un sac contenant un ordinateur et des données personnelles dans le métro, ayant entraîné une violation de données.

✅ Bonnes pratiques en matière de sécurité de l'informatique mobile

- Authentifier les utilisateurs à l'ouverture de session (cf. partie précédente).
- Mettre en œuvre des mécanismes de sauvegardes ou de synchronisation.
- Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes etc).
- Lors de vos déplacements, privilégiez l'utilisation de connexions à des réseaux sécurisés et fiables, de préférence ceux que vous connaissez. À défaut, optez pour le partage de connexion via votre mobile. Évitez absolument les réseaux Wi-Fi publics, qui présentent des risques majeurs pour la sécurité de vos données.
- Pour préserver la confidentialité de vos travaux, évitez de travailler dans des lieux publics ou dans les transports. En cas d'impossibilité, utilisez des filtres de confidentialité sur vos écrans afin de vous protéger des regards indiscrets.

🔍 FOCUS : protéger ses données en cas de départ à l'étranger

Outre les mesures listées ci-dessus, lors de déplacements à l'étranger, il est parfois nécessaire de prendre des mesures de sécurité spécifiques pour protéger vos équipements et vos données, car les risques d'espionnage industriel ou de confiscation de matériel par les autorités locales sont bien réels :

- Voyager léger en données : Emportez uniquement les informations strictement nécessaires à votre mission. Limitez les données personnelles ou sensibles autant que possible. Rappelez-vous que dans les pays hors UE, le RGPD ne s'applique pas, et vos données seront soumises à la législation locale.
- Appareils sécurisés : Préférez un smartphone "propre", dépourvu de données sensibles, spécifiquement réservé à ce type de déplacement. Utilisez un ordinateur avec un disque dur vierge, contenant uniquement les fichiers requis pour votre mission. Si possible, empruntez un appareil dédié pour les voyages à l'étranger.
- Utilisation d'un VPN : Dans les pays à risque en matière de vie privée, téléchargez et utilisez un VPN avant de partir pour protéger vos connexions et contourner une éventuelle censure ou surveillance.
- Authentification renforcée : Activez la double authentification sur tous vos comptes avant votre départ et conservez vos codes de secours dans un endroit hors ligne.
- Mots de passe temporaires : Modifiez vos mots de passe avant votre départ et changez-les de nouveau à votre retour. Cette précaution est essentielle, car certaines autorités locales pourraient vous demander l'accès à vos appareils pour inspection.
- Désactivation de la biométrie : Désactivez les fonctionnalités de reconnaissance faciale et d'empreintes digitales sur vos appareils afin de limiter les risques de contournement ou d'abus en cas de confiscation.

3) Conserver les données

Organiser les modalités de conservation : Toute utilisation de données personnelles dans un cadre de recherche suppose d'avoir **anticipé** les modalités d'utilisation qui en seront faites.

✅ Bonnes pratiques en matière de conservation

- Définissez des durées de conservation adaptées aux objectifs poursuivis (cf. fiche 10) et mettez en place des alertes, archivages ou purges automatisées.
- Effectuez des sauvegardes régulières des données papier et électroniques, et testez leur fiabilité (cf. fiche 9) pour éviter toute perte ou altération.
- Utilisez des supports de stockage sécurisés en évitant les services de cloud grand public hébergés hors UE, ainsi que les clés USB et disques durs externes non protégés. Privilégiez le chiffrement[8] pour assurer la confidentialité des données sensibles (cf. fiche 9).

Garantir la confidentialité : Que les données utilisées pour la réalisation des travaux de recherche soient au format papier (carnets d'enquêtes, notes d'entretiens, questionnaires, etc.) ou numérique, il est nécessaire de s'assurer que seules les personnes autorisées sont en mesure d'y accéder. Si des tiers parviennent à y accéder (même uniquement en consultation), **cela constituerait une violation de données dont vous seriez responsable, ce qui pourrait entraîner des sanctions**.

✅ Bonnes pratiques en matière de confidentialité

Au niveau informatique :

[8] https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

- En fonction de la sensibilité des données, mise en place d'un chiffrement conformément aux recommandations de l'ANSSI [9], pour garantir la sécurité des données (méthodes de chiffrement et des clés de taille appropriée, conservation des clés de chiffrement...).
- Prévoir une procédure de verrouillage automatique de session et verrouiller son ordinateur dès que l'on quitte son poste de travail en utilisant les raccourcis clavier Windows+L ou Crtl+Commande+Q.

Au niveau physique : Il est essentiel de garantir la sécurité des accès aux locaux où sont stockées les données utilisées dans le cadre de la recherche (bureaux, salles serveurs, etc.). Cela inclut :

- La mise en place de mesures telles que l'accompagnement des visiteurs, l'utilisation de badges d'accès et/ou l'installation de portes verrouillées.
- Ranger et sécuriser les documents contenant des données personnelles utilisées pour les travaux de recherche, en évitant de les laisser sans surveillance sur un bureau ou dans un véhicule. Les données scientifiques sous format papier doivent normalement être conservées dans des espaces et équipements sécurisés, tels qu'une armoire ou un coffre-fort fermé. Seules les personnes habilitées doivent avoir l'accès à ces espaces, via une clé, un code ou un badge, afin de préserver la confidentialité et l'intégrité des informations.

4) Superviser la diffusion des données

Sécuriser les échanges : La réalisation de travaux de recherche en partenariat peut nécessiter la réalisation d'échanges de données entre différentes équipes. Comme expliqué précédemment, **une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités et à porter ainsi atteinte au droit à la vie privée des personnes**.

✅ Bonnes pratiques en matière de sécurisation des échanges

- Chiffrez les fichiers sensibles avant toute transmission numérique. Il en va de même pour les supports physiques (clés USB, disques durs portables, etc.), qui doivent être chiffrés avant d'être remis en main propre, confiés à un coursier ou par voie postale.
- Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).
- Certains organismes employant les personnels de recherche peuvent également proposer la mise à disposition de plateformes sécurisées spécialement dédiées aux échanges de données. Il est recommandé dans ce cas de recourir autant que possible à ces ressources.

📌 Exemples de sécurisation des échanges

L'Université Paris 1 vous propose, via votre espace ENT [10], le service « FILEX » pour l'envoi sécurisé de fichiers volumineux. Ce service offre la possibilité de définir un mot de passe ou d'exiger une authentification pour garantir la sécurité des transferts.
Si vous êtes à l'aise avec GitHub, vous pouvez également explorer « Eurydice », une solution open source développée par l'ANSSI, qui permet de transférer des informations de manière sécurisée entre deux réseaux de niveaux de sécurité différents [11].

[9] https://cyber.gouv.fr/publications/mecanismes-cryptographiques
[10] https://filex-ng.univ-paris1.fr/
[11] https://github.com/ANSSI-FR/eurydice/blob/master/README.md

Canaux de transmission : Il est également nécessaire de veiller à la sécurité des données lors des **échanges en dehors des espaces de travail collaboratif** :

✅ Bonnes pratiques en matière de transmission des données

- Utilisez le chiffrement de vos données sensibles AVANT l'envoi ou vérifiez si l'application que vous utilisez propose cette fonctionnalité. Cela permet de garantir que les informations restent confidentielles pendant leur transmission.
- Si cela n'est pas possible, assurez-vous a minima que l'accès aux documents est protégé par un mot de passe, afin de limiter leur consultation uniquement aux personnes autorisées.
- Envisagez d'ajouter des filtres ou des filigranes sur vos documents, comme avec des outils tels que Filigrane Facile [12] afin d'éviter le vol ou la réutilisation des données.
- Bannissez la transmission de fichiers contenant des données personnelles en clair via des messageries « grand public » non sécurisées.
- Rappel : privilégiez l'utilisation de connexions à des réseaux sécurisés et fiables, de préférence ceux que vous connaissez. À défaut, optez pour le partage de connexion via votre mobile. Évitez absolument les réseaux Wi-Fi publics, qui présentent des risques majeurs pour la sécurité de vos données.

Encadrer le partage et/ou la publication : La diffusion de jeu de données ayant permis la réalisation de travaux de recherche est de plus en plus demandée aux personnels de recherche (revue par les pairs, publication de résultats dans une revue scientifique...). **Ces prérogatives de science ouverte doivent cependant s'accorder avec les impératifs de protection des données**.

✅ Bonnes pratiques en matière de partage et de publication

Anonymiser les données permet de les sortir du cadre de la protection des données personnelles, car les données anonymisées ne sont plus considérées comme personnelles. Cependant, cette opération implique souvent une perte significative d'informations, ce qui peut être problématique pour certains travaux de recherche. Si l'anonymisation n'est pas envisageable, la pseudonymisation constitue une alternative intéressante et moins contraignante. Elle permet de réduire les risques liés à l'identification tout en préservant l'intégrité des données. Contrairement à l'anonymisation, la pseudonymisation peut être mise en place de manière plus simple et avec moins de pertes d'informations pour le chercheur, puisque les données restent associées à un identifiant codé qui peut être réutilisé dans le cadre des travaux scientifiques. De plus, la pseudonymisation doit être systématiquement appliquée avant toute publication (thèse, articles scientifiques, etc.) pour garantir le respect des exigences de confidentialité et de protection des données personnelles.

🔍 FOCUS : Anonymisation VS Pseudonymisation

L'anonymisation et la pseudonymisation sont deux techniques de protection des données personnelles, mais elles ne garantissent pas le même niveau de protection. L'anonymisation vise à rendre impossible toute réidentification d'une personne à partir des données traitées, même en croisant différentes sources d'information. En pratique, c'est un processus rare et complexe, car

[12] https://filigrane.beta.gouv.fr/

il est très difficile de garantir qu'aucune donnée résiduelle ne permettrait de remonter à une personne, notamment avec l'évolution des technologies et des capacités de corrélation des données.
À l'inverse, la pseudonymisation consiste à remplacer les éléments identifiants par un code ou un alias, tout en conservant une possibilité de réassociation avec l'identité réelle via une clé de correspondance. Une donnée est également considérée comme pseudonymisée lorsqu'il subsiste un risque de réidentification par recoupement avec d'autres informations (âge, parcours, réponses spécifiques à un questionnaire, etc.). Ainsi, si la pseudonymisation réduit les risques en limitant l'identification directe des personnes concernées, elle ne les rend pas anonymes pour autant.

Quelles sont les mesures de sécurité organisationnelles ?

Les mesures organisationnelles englobent **l'ensemble des politiques, procédures et méthodes établies** pour assurer une gestion appropriée des données personnelles. Elles ne remplacent en aucun cas les mesures techniques, mais viennent plutôt les compléter pour renforcer la protection des données.

Tout comme pour les mesures techniques, cette liste présente les principales mesures organisationnelles que vous pouvez mettre en place. Elle n'est cependant pas non plus exhaustive.

- **Analyse d'impact sur la protection des données** : Dans le cadre du traitement de données sensibles, une AIPD a-t-elle été planifiée conformément à l'article 35 du RGPD ? (cf. fiche pratique 14).

- **Formations** : Le chercheurs membres de l'équipe ont-ils été sensibilisés aux obligations et enjeux de la protection des données personnelles ? Si oui, qui a réalisé cette formation et à quelle date ? Ont-ils tous signé des engagements de confidentialité ?

- **Contrôle des sous-traitants** : Un encadrement des sous-traitants et prestataires manipulant des données personnelles a-t-il été prévu ? Cela inclut-il des contrats mentionnant la protection des données et des engagements de confidentialité ?

- **Politique de sécurité informatique** : Existe-t-il une politique de sécurité informatique au sein de votre laboratoire ou unité, et celle-ci est-elle appliquée ? Si oui, vous devez respecter et vous appuyer sur les textes et mesures internes de votre établissement.

- **Procédures de gestion des données** : Y a-t-il des procédures pour détecter, signaler et répondre aux violations de données ? Des vérifications régulières sont-elles effectuées pour garantir le respect et l'efficacité des mesures de sécurité ?

- **Comité d'éthique** : Le comité d'éthique de l'université ou d'un autre organisme a-t-il été consulté ? Quelle a été sa réponse ?

Que dois-je indiquer dans la fiche du registre ?

Tout comme cette fiche, le registre inclut une section dédiée à la « **Sécurité des données (technique)** » suivie d'une section sur la « **Sécurité des données (organisationnelle)** ».

Dans la première section, vous pourrez remplir deux champs concernant la méthode d'authentification et le chiffrement des données. Si vous avez des doutes sur l'authentification, vous pouvez laisser ce champ vide, tandis que pour le chiffrement, vous aurez l'occasion de fournir des détails plus précis par la suite.

Je vous encourage à énumérer toutes les mesures de sécurité techniques que vous avez identifiées dans le champ « **Autres précisez** », ce qui vous permettra de développer votre travail. Vous pouvez présenter ces mesures sous forme de liste à puces organisée par actif, comme indiqué dans cette fiche, ou selon une autre structure de votre choix.

De même, vous pourrez répertorier toutes les mesures organisationnelles mises en place dans le champ libre prévu à cet effet.

✅ Bonnes pratiques et recommandations d'hygiène numérique

L'application des mesures techniques et organisationnelles mentionnées ci-dessus doit être complétée par des bonnes pratiques essentielles, qui restent fondamentales pour garantir la sécurité.
- Restez vigilant(e) lors de votre navigation sur Internet en évitant les sites non sécurisés ou douteux. Privilégiez toujours les sites en HTTPS pour vous protéger contre les infections par des logiciels malveillants.
- Téléchargez uniquement des logiciels et applications depuis les sites officiels des constructeurs. Cela vous permet d'éviter les programmes modifiés ou corrompus, assurant ainsi une meilleure sécurité pour vos données.
- Ne cliquez jamais sur des liens suspects ou malveillants envoyés par email. Une seule erreur peut entraîner une attaque par phishing ou l'installation d'un logiciel malveillant. Prenez quelques secondes pour vérifier l'origine du message, l'expéditeur, et survolez les liens sans cliquer pour lire l'adresse complète avant de valider.
- Évitez d'insérer des clés USB qui ne vous appartiennent pas, que vous les ayez trouvées, empruntées ou reçues en cadeau. Ces supports peuvent contenir des virus et des malwares susceptibles de compromettre la sécurité de votre ordinateur.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Sécurité des données (technique)** incluant les champs **Authentification**, **Données chiffrées** et **précisions**.
- **Sécurité des données (organisationnelle)**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 12 : Exporter des données hors de l'Union Européenne

Qu'est-ce qu'un « transfert de données » ?

Un « **transfert de données** » désigne toute transmission, quel que soit le moyen utilisé, de données personnelles depuis un pays de l'Union Européenne (UE) vers un pays situé en dehors de cet espace.

Vous êtes par exemple concerné(e) par un transfert de données dans le cadre de votre projet de recherche si :
- Vous collaborez avec un partenaire de recherche basé dans un pays extérieur à l'UE.
- Vous utilisez un outil, une application ou un service informatique dont les serveurs sont situés hors de l'UE (messagerie, stockage, analyse de données, etc.).
- Vous faites appel à un sous-traitant ou prestataire basé en dehors de l'UE, ou disposant de centres de traitement dans un pays tiers.

⚠ Attention

Le transfert ne se limite pas aux données envoyées intentionnellement à l'étranger. Même si les données sont physiquement hébergées dans l'UE, elles peuvent être considérées comme transférées si un destinataire situé en dehors de l'UE y accède à distance. Comme précisé, cette situation est fréquente lors de l'utilisation de services informatiques proposés par des entreprises non européennes.

Comment déterminer si je réalise un transfert de données ?

Un traitement est considéré comme un transfert de données hors de l'Union européenne si les trois critères suivants sont remplis simultanément :

1) **L'exportateur des données doit être soumis au RGPD**, qu'il soit situé dans l'UE ou pas, par exemple : le chercheur, le laboratoire ou l'université situé dans l'UE qui traite les données personnelles. Idem si l'entité de recherche est hors UE mais cible des personnes dans l'UE (ex. participation à un projet européen, collaboration avec une université européenne), elle peut aussi être soumise au RGPD.

2**) Les données sont communiquées ou rendues accessibles à un destinataire situé hors de l'UE** : Il y a transfert si les données issues des recherches sont envoyées, partagées ou accessibles par une institution, un chercheur ou un partenaire basé en dehors de l'UE/EEE.

3) **Le destinataire est une entité distincte de l'exportateur et située dans un pays tiers** : Le transfert implique que les données soient mises à disposition d'un autre organisme, chercheur ou institution située hors de l'UE/EEE.
Cela signifie que si un chercheur d'une université européenne consulte uniquement des données hébergées dans l'UE depuis l'étranger sans les partager avec une autre entité, ce n'est pas considéré comme un transfert.

Si ces trois conditions sont remplies, cela signifie que vous êtes bien concerné par un transfert de données hors de l'UE, auquel cas, les recommandations suivantes vous aideront à encadrer juridiquement ce transfert.

Pourquoi faut-il s'intéresser à la mise en conformité du transfert de données à l'étranger ?

Le RGPD impose un encadrement strict des transferts de données personnelles vers des pays situés en dehors de l'UE afin de garantir un niveau de protection adéquat pour les personnes concernées, même lorsque les données quittent le territoire européen. Cette exigence découle du fait que **les règles de protection des données varient d'un pays à l'autre**, et **certains pays n'offrent pas une protection équivalente à celle de l'UE**.

Si un transfert de données n'est pas correctement encadré, les données personnelles peuvent être exposées à des risques accrus : utilisation non conforme, perte de confidentialité, failles de sécurité, ou encore obligations légales locales incompatibles avec les exigences du RGPD. En veillant à respecter les règles applicables aux transferts, vous contribuez à protéger les droits des personnes concernées et à minimiser les risques juridiques liés à votre projet. Avant de procéder à un transfert, il est donc indispensable de vérifier si le pays de destination offre des garanties suffisantes de protection des données (nous expliquerons plus en détail comment procéder dans les sections suivantes).

Puis-je transférer des données au sein de l'UE et/ou en dehors ?

Le RGPD autorise les transferts de données personnelles en dehors de l'UE à condition de garantir un niveau de protection suffisant et approprié des données. Cela implique de vérifier, au cas par cas, si la législation du pays de destination assure une protection équivalente ou supérieure à celle du RGPD.

Transferts au sein de l'UE : Les transferts de données personnelles au sein de l'UE ne posent pas de difficulté particulière, car tous les pays membres appliquent le même niveau de protection des données prévu par le RGPD. Ainsi, ces transferts peuvent se faire librement, sans analyse ni formalité supplémentaire.

Transferts en dehors de l'UE : Le RGPD considère les transferts hors de l'UE comme risqués par défaut et les interdit, sauf si l'une des solutions suivantes permet de garantir la protection des données :
- **Décision d'adéquation** (le cas simple) : Si la Commission européenne a adopté une décision d'adéquation pour un pays tiers, cela signifie que ce pays offre un niveau de protection des données équivalent à celui de l'UE (article 45 du RGPD). Dans ce cas, le transfert est autorisé sans formalités supplémentaires.
- **Garanties appropriées via des clauses contractuelles types** (cas plus complexe) : Si aucun accord d'adéquation n'existe, il est possible de transférer des données en utilisant des garanties appropriées, comme les clauses contractuelles types. Ces clauses, fournies par la Commission européenne, doivent être intégrées dans les contrats avec les destinataires étrangers des données. Cette solution est plus complexe, car elle demande une formalisation rigoureuse des conditions de transfert.
- **Consentement explicite des personnes concernées** (cas exceptionnel) : En l'absence d'une décision d'adéquation ou de garanties appropriées, un transfert peut être effectué si les

personnes concernées donnent leur consentement explicite, après avoir été informées des risques liés au transfert. Cette solution doit rester exceptionnelle et ne s'applique qu'aux transferts ponctuels (article 49 du RGPD).

À retenir : Un transfert de données personnelles hors UE n'est autorisé que si l'une de ces trois solutions est mise en œuvre. Dans le cas contraire, le transfert est illégal, et votre responsabilité pourra être engagée. Soyez donc vigilant, si vous envisagez un tel transfert, contactez rapidement votre DPO pour vérifier ensemble la conformité et garantir que les exigences réglementaires sont bien respectées.

Cas 1 : Comment savoir si mon transfert est concerné par une décision d'adéquation ?

Comme expliqué précédemment, la décision d'adéquation adoptée par la Commission européenne (art. 45 du RGPD), constitue le premier outil juridique d'encadrement, dans la mesure où elle est prise sur la base d'un examen global de la législation en vigueur dans un État, sur un territoire ou applicable à un ou plusieurs secteurs déterminés au sein de cet État.

Pour vérifier si un pays bénéficie d'une décision d'adéquation, rendez-vous simplement sur le site de la CNIL, rubrique « La protection des données dans le monde » : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde. Recherchez-le ou les pays concernés par le transfert sur la carte du monde (une loupe est à votre disposition pour rentrer vous-même le nom du pays).

Voici les résultats possibles :
- **Pays membre de l'UE ou de l'EEE** : La protection des données y est déjà encadrée par le RGPD. Aucune formalité particulière n'est requise.
- **Pays reconnu comme adéquat** : L'UE considère que ce pays offre un niveau de protection équivalent au RGPD. Le transfert est autorisé sans formalité supplémentaire.
- **Pays partiellement adéquat** : Ce pays est reconnu comme adéquat uniquement pour certains types de traitements. Le site de la CNIL précise lesquels. Si votre transfert ne correspond pas aux traitements autorisés, il faudra envisager les solutions des cas 2 ou 3.
- **Pays non reconnu comme adéquat** : Ce pays n'offre pas un niveau de protection suffisant selon l'UE. Vous devrez impérativement examiner les alternatives prévues dans les cas 2 et 3.

Pour rappel, si le transfert est autorisé sans formalisme supplémentaire, vous pouvez poursuivre la lecture de cette fiche en sautant l'étude des deux prochaines exceptions. En revanche, si le pays n'est pas adéquat ou seulement partiellement adéquat, étudiez les solutions des cas 2 et 3 pour encadrer le transfert.

Cas 2 : Qu'est-ce que des clauses contractuelles types et comment les mettre en place ?

En l'absence d'une décision d'adéquation, il est possible de s'appuyer sur des « *garanties appropriées* » (art. 46 du RGPD), constituées pour la majorité de mécanismes contractuels. Ces garanties peuvent notamment consister en des clauses types de protection des données adoptées par la Commission européenne. Ces **clauses contractuelles types** (CCT) sont des dispositions standard servant à encadrer juridiquement les transferts de données personnelles vers des pays ne disposant pas d'une décision d'adéquation. En clair, ces clauses garantissent que **le destinataire des données hors UE respecte des obligations similaires à celles du RGPD**, protégeant ainsi les droits et libertés des personnes concernées.

📌 **Exemple**

Si une recherche est menée conjointement entre une équipe de recherche française et une équipe de recherche brésilienne, un transfert de données hors de l'UE pourra être réalisé par l'utilisation de clauses contractuelles type de la Commission européenne.

Ces clauses permettent de formaliser un transfert de données en créant un cadre juridique contraignant pour la partie destinataire. Elles fixent notamment les obligations des deux parties :
- La partie exportatrice (celle qui transfère les données) doit s'assurer que les données sont correctement protégées avant le transfert.
- La partie importatrice (celle qui reçoit les données) doit s'engager à respecter des standards élevés de protection des données et permettre des contrôles réguliers si nécessaire.

Paris 1 est actuellement en phase d'apprentissage et de mise en œuvre de ces CCT. Comme elles doivent être adaptées en fonction du type de relation entre les parties (par exemple : transfert entre deux responsables de traitement ou entre un responsable de traitement et un sous-traitant), chaque cas doit être étudié avec attention.

Mettre en place des clauses contractuelles types demande de formaliser un contrat ou une convention entre les deux parties comprenant : une annexe d'environ 20 pages contenant les clauses standard fournies par la Commission européenne, ainsi que la rédaction de plusieurs pages décrivant précisément le traitement des données (cela ressemble beaucoup aux informations que vous apprenez à inscrire dans le registre).

Si vous êtes concerné(e) par un transfert de données hors UE et que votre DPO pense que les CCT peuvent être une solution à votre situation, il vous aidera alors à examiner la faisabilité du transfert et la mise en place des clauses adaptées.

Cas 3 : Comment utiliser le consentement des personnes en dernier recours ?

En l'absence de décision d'adéquation (cas 1) et de garanties appropriées (cas 2), le transfert peut toujours être réalisé sur **la base de dérogations** (art. 49 RGPD) dans des situations particulières et des conditions spécifiques. Le **consentement des personnes** concernées peut constituer une solution légale pour un transfert de données hors de l'UE.

⚠ Attention

Ces exceptions ne peuvent pas fonder des transferts de données massifs, systématiques ou sur des grands ensembles de données. Il est donc essentiel que ce recours reste exceptionnel en cas de transfert non répété, car un transfert régulier fondé uniquement sur le consentement serait contraire aux exigences du RGPD.

Le consentement doit être donné librement, de manière explicite et après que les personnes concernées ont été pleinement informées des risques associés au transfert. Cela signifie que les individus doivent comprendre les conséquences potentielles d'un transfert vers un pays dont la législation n'offre pas un niveau de protection équivalent au RGPD. Ainsi, avant de demander le consentement, une analyse de risque du transfert doit être réalisée en collaboration avec le DPO.

L'information sur ce transfert et ses risques devra figurer dans les mentions d'information obligatoires (cf. fiche pratique 8). Toutefois, il est recommandé d'aller au-delà de cette simple mention et de fournir un document distinct, spécifique à la question du transfert, expliquant clairement : les finalités du transfert, les pays concernés, les destinataires et les risques

identifiés. Cette démarche vise à garantir que les personnes comprennent pleinement les enjeux de leur consentement. Une fois de plus, soyez vigilant(e), car votre responsabilité pourrait être engagée si les personnes concernées ont donné leur consentement à participer à vos recherches sans être pleinement informées de cet aspect.

📌 Exemple

Si une équipe de recherche souhaite transférer des données personnelles à une autre équipe située dans un pays tiers n'offrant pas un niveau de protection des données jugé adéquat, et qu'aucune garantie appropriée ne peut être mise en place pour encadrer ce transfert, il reste possible, à titre exceptionnel, d'effectuer le transfert. Cette exception s'applique uniquement si toutes les personnes concernées ont donné leur consentement explicite après avoir été pleinement informées des risques que ce transfert pourrait représenter pour elles (cf. article 49.1.a du RGPD).

Que dois-je indiquer dans la fiche du registre ?

À ce stade, vous avez tous les éléments nécessaires pour compléter les champs du registre de traitement. Dans la section « **Destinataires des données** », répondez « Oui » ou « Non » à la question « **Transfert de données hors de l'UE** ».

Ensuite, pour la question suivante, concernant le « **Détail transfert** », renseignez les informations suivantes :
- Liste des pays concernés : indiquez s'ils font partie de l'UE ou non.
- Statut de conformité selon la CNIL : mentionnez si le pays est adéquat, partiellement adéquat ou non adéquat.
- Justification du transfert : précisez les raisons pour lesquelles vous effectuez ce transfert.
- Destinataires dans le pays concerné : identifiez précisément les destinataires externes localisés à l'étranger. Assurez-vous que votre liste des destinataires externes précédemment complétée dans le registre soit bien à jour.
- Instrument juridique autorisant le transfert : pour chaque transfert, indiquez l'instrument juridique appliqué : décision d'adéquation (cas 1), mise en place de CCT (cas 2) ou consentement (cas 3).
- Mesures de sécurité : n'oubliez pas de détailler les mesures de sécurité mises en place pour assurer la protection des données pendant le transfert (telles que le chiffrement par exemple).

Si vous êtes concerné par un cas d'importation de données, dans la section « **Données traitées** », vous devrez compléter la question relative à la « **Méthode de collecte des données** ». Précisez clairement la source des données importées de l'étranger, qu'il s'agisse d'un organisme public, d'une institution, des personnes concernées directement (par exemple, à travers des entretiens), ou de tout autre moyen.

Enfin, vous pouvez ignorer les champs « **Possibilité d'extractions locales** » et « **Détail extractions locales** ».

🔍 FOCUS : Importer des données personnelles depuis l'étranger : quelles démarches et précautions à prendre ?

L'importation de données au sein de l'Union européenne pose généralement moins de difficultés que leur exportation. En effet, le RGPD s'applique automatiquement aux données traitées sur le territoire de l'UE. Ainsi, les données importées dans l'UE sont directement soumises à ses règles. Ce processus d'importation est relativement simple et se déroule en deux étapes :
1) Garantir la conformité au RGPD : cela implique de remplir les formalités nécessaires, notamment la déclaration du traitement et la tenue d'une fiche dans le registre de traitement.
2) Dans un second temps : vous devez vous assurer que vous respectez bien les conditions de transfert imposées par le pays tiers. Autrement dit, bien que les données soient soumises au RGPD une fois sur le territoire européen, vous devez vérifier si le pays d'origine impose des conditions spécifiques pour le transfert de données vers l'UE. Il s'agit de l'exercice inverse de celui que nous avons effectué précédemment pour les transferts sortants. Vous devrez donc comparer les exigences légales du pays exportateur avec celles de l'UE pour vous assurer que toutes les conditions nécessaires sont respectées (ce processus est généralement une formalité relativement simple).

Pour vous aider dans cette démarche, vous pouvez consulter le site DLA Piper Data Protection, où vous pourrez rechercher le pays d'origine des données et examiner les exigences locales : https://www.dlapiperdataprotection.com/
La section "Transfert" de chaque pays vous donnera les informations nécessaires pour savoir si des formalités spécifiques sont requises avant de procéder à l'importation des données.

En cas de doute, ou si les données proviennent de pays dans des situations sensibles (par exemple, en temps de guerre ou de crise), il est fortement recommandé de contacter votre DPO. Dans ce type de situation, des mesures de sécurité supplémentaires peuvent être nécessaires pour protéger les données et les droits des personnes concernées.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Transfert de données hors de l'UE**
- **Détail transfert**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 13 : Sous-traitance

Qu'est-ce que la sous-traitance ?

Dans le cadre du RGPD, la sous-traitance désigne le fait de confier à un tiers, appelé sous-traitant, tout ou partie du traitement de données personnelles. Il s'agit d'une personne physique ou morale que vous mandatez pour effectuer un traitement en votre nom et pour votre compte.

Quelle importance me concernant ?

Lorsque vous faites appel à un prestataire pour traiter des données personnelles, il ne suffit pas de lui faire confiance sans formaliser juridiquement la relation. En tant que responsable de traitement, le RGPD vous impose de vous assurer que votre sous-traitant respecte bien ses obligations en matière de protection des données. En cas de manquement, notamment en matière de sécurité ou en cas de violation de données, **vous restez responsable, même si la faute incombe au prestataire**. Un encadrement rigoureux de la sous-traitance est donc essentiel pour protéger votre responsabilité et garantir la conformité de vos traitements.

✅ **Bonnes pratiques : formaliser la sous-traitance par un contrat**

La sous-traitance doit être formalisée par un contrat conforme à l'article 28 du RGPD, précisant notamment la gestion des données personnelles, la durée et la nature des traitements, ainsi que les mesures de sécurité mises en place. Ce contrat est aussi l'occasion d'intégrer une clause de confidentialité. Si celle-ci n'a pas été prévue dès la signature, elle peut être complétée par un engagement de confidentialité, disponible en ANNEXE 1 : LIEN ICI.

Si vous avez besoin de modèles types de clauses sur la sous-traitance, n'hésitez pas à contacter votre DPO, qui pourra vous les fournir.

Comment savoir si je suis concerné(e) par la sous-traitance ?

Dans le cadre de vos travaux et projets de recherche, vous pouvez être amenés à faire appel à des prestataires ou partenaires externes pour divers services. Pour déterminer si une relation relève de la sous-traitance au sens du RGPD, deux critères principaux s'appliquent :

- Si vous confiez un traitement de données personnelles à un prestataire (par exemple, la réalisation d'une enquête, le développement d'un site internet ou l'analyse de données) et qu'il agit pour accomplir une tâche spécifique pour vous, et non pour ses propres besoins, il s'agit d'une sous-traitance.
- Si un contrat de prestation a été signé avec un prestataire, définissant son rôle, ses missions et les services qu'il s'engage à fournir, il y a de fortes chances qu'il s'agisse également d'un sous-traitant au sens du RGPD.

Que dois-je indiquer dans la fiche du registre ?

Dans la section « **Sous-traitance** », plusieurs champs vous permettent de préciser cette relation :

- **Sous-traitance** : Indiquez si votre projet implique ou non une prestation de sous-traitance.
- **Détails** : Précisez les informations essentielles, telles que l'identité du prestataire ou de sa société, son rôle et sa finalité d'intervention, les données auxquelles il aura accès et la durée prévue de la prestation.
- **Convention(s) ou contrat(s)** : Téléchargez ici le contrat ou l'accord encadrant la relation avec le prestataire.

Vous ne pouvez malheureusement ajouter qu'un seul sous-traitant. Si vous en avez plusieurs, numérotez-les et divisez les informations dans le champ « **Détails** » et vous pourrez fusionner les documents pour regrouper les conventions ensemble.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :

- **Sous-traitance**
- **Détails**
- **Convention(s) ou contrat(s)**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

Fiche 14 : Analyse d'impact relative à la protection des données

Qu’est-ce qu’une Analyse d'Impact relative à la Protection des Données (AIPD) ?

L’AIPD est une démarche d’évaluation des risques visant à accompagner les responsables de traitement dans la conception de traitements de données respectueux de la vie privée et conformes au RGPD. Elle est **obligatoire pour les traitements susceptibles de présenter un risque élevé pour les droits et libertés des personnes concernées**, en particulier lorsqu’ils traitent des données sensibles.

Réaliser une AIPD sert à **évaluer les risques qu'un traitement de données personnelles peut faire peser sur les personnes concernées et de s'assurer que des mesures de sécurité adaptées sont mises en place pour les protéger**. C'est une façon de prévenir les problèmes avant qu'ils ne surviennent et de prouver que le traitement respecte les règles du RGPD. Cela permet aussi d'éviter des incidents ou des sanctions qui pourraient nuire à un projet ou à une organisation.

Quand dois-je réaliser une AIPD ?

Conformément à l’article 35 du RGPD, « *Lorsqu’un type de traitement [...]* ***est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes*** *physiques, le responsable du traitement effectue, avant le traitement, une analyse de l’impact des opérations de traitement envisagées sur la protection des données à caractère personnel* ».

Pour déterminer si un traitement présente un risque élevé, il ne s’agit pas d’une appréciation subjective, mais d’un examen fondé sur des critères objectifs et précis. Voici quelques situations courantes dans lesquelles une AIPD devient nécessaire :

- **Traitement de catégories particulières de données « sensibles** » : Un projet de recherche en SHS pourrait consister à étudier des données sur la santé, les opinions politiques, les croyances religieuses ou encore les infractions pénales.
- **Traitement concernant des personnes vulnérables** : Cela inclut les enfants, les malades, les personnes âgées ou encore les détenus.
- **Traitement de données à grande échelle** : Un traitement est considéré comme de grande échelle lorsqu’il concerne un très grand volume de données ou un grand nombre de personnes. En SHS, cela pourrait être le cas d’une enquête nationale collectant des milliers de réponses sur les conditions de vie des étudiants.
- **Croisement ou combinaison de données provenant de différentes sources** : Si un projet consiste à combiner des données issues d’enquêtes, de bases administratives et de réseaux sociaux pour étudier un phénomène social, cela peut créer un risque élevé en raison de la richesse des informations obtenues.
- **Limitation des droits des personnes concernées** : Certains traitements peuvent limiter l’accès à un service ou à un droit. Par exemple, dans une étude sur les comportements déviants, le refus de participation pourrait entraîner l’exclusion d’un programme d’aide ou de réinsertion.
- **Prise de décision automatisée** : Lorsqu’un traitement aboutit à des décisions automatisées ayant des effets importants sur les personnes, comme un algorithme décidant de l’attribution de bourses sur la base de critères sociaux.

- **Surveillance systématique des personnes** : Cela peut concerner la collecte régulière d'images ou de données comportementales dans un cadre expérimental. Par exemple, filmer en continu des participants lors d'une expérience d'interaction sociale en laboratoire.
Etc...

Si votre traitement répond <u>à au moins deux de ces critères</u>, une AIPD doit être réalisée avant de commencer à collecter et exploiter les données. Cette analyse permet d'identifier les risques pour les personnes concernées, tels que des accès non autorisés ou des modifications de données, et de définir les mesures nécessaires pour garantir la protection de leurs données personnelles.

📌 **Exemples de traitements de données personnelles à finalité de recherche scientifique pour lesquels une AIPD devrait être réalisée** :

- Une enquête visant à interroger des personnes détenues et à recueillir des données sur leurs pratiques religieuses (personnes vulnérables et données sensibles) ;
- Une collecte de données personnelles sur les réseaux sociaux dans le cadre d'une recherche sociologique afin de générer des profils d'usagers (évaluation, grande échelle, croisement de données) ;
- Une recherche visant à développer un algorithme de reconnaissance du locuteur par ses caractéristiques vocales chez des enfants en les enregistrant (données sensibles, personnes vulnérables).

Comment réaliser une AIPD ?

L'AIPD vise à identifier et anticiper les risques pouvant compromettre l'intégrité, la confidentialité ou la disponibilité des données personnelles :
- **Perte d'intégrité** : modification non désirée des données.
- **Perte de disponibilité** : impossibilité d'accéder aux données.
- **Perte de confidentialité** : accès non autorisé aux données.

Les risques pouvant entraîner ces situations sont variés, tels que :
- Perte ou vol de matériel informatique : ordinateur, téléphone portable, tablette, etc.
- Espionnage ou ingérence étrangère lors de déplacements à l'étranger.
- Accident naturel : inondation, incendie, tempête...
- Erreur humaine : mauvaise manipulation, suppression involontaire.
- Actes malveillants intentionnels : destruction, modification ou diffusion des données par un membre interne de l'équipe.
- Fuite de données chez le prestataire ou l'hébergeur des données.

Si votre traitement de données répond à au moins deux critères nécessitant une AIPD, contactez rapidement votre DPO. Celui-ci vous fournira un modèle d'AIPD (généralement sous forme d'un document Word) à remplir. Ce document vous demandera d'identifier les risques possibles, d'envisager des scénarios critiques et de prévoir des solutions pour réduire ces risques.

Votre DPO vous accompagnera dans cette démarche. Toutefois, vous devriez être en mesure de réaliser une grande partie de l'AIPD de façon autonome, notamment si vous avez déjà complété

le registre de traitement : les informations que vous y avez renseignées vous seront très utiles pour cette analyse de risque.

Comment remplir la fiche du registre de traitement ?

Dans la section « **Données traitées** », vous trouverez une dernière ligne intitulée « **Risques et impacts sur la vie privée** ». Une fois votre AIPD finalisée et validée par votre DPO, vous pourrez y déposer le fichier correspondant.

Comme l'analyse d'impact peut nécessiter du temps, en attendant sa finalisation, vous pouvez mentionner parmi les mesures de sécurité organisationnelles qu'une AIPD est en cours de réalisation » (cf. fiche pratique 11). Cela permettra de montrer que vous êtes en train de prendre en compte les risques liés à votre traitement de données.

🎯 Récapitulatif

À la fin de cette fiche pratique, vous devriez être en mesure de compléter les éléments suivant dans votre fiche du registre des traitements :
- **Risques et impacts sur la vie privée**

Si ce n'est pas le cas ou si vous avez des questions, n'hésitez pas à nous contacter à l'adresse suivante : dpo@univ-paris1.fr

ANNEXE 1 : Engagement de confidentialité

ENGAGEMENT DE CONFIDENTIALITÉ

Cet engagement s'adresse aux personnes externes amenées à manipuler des données personnelles appartenant à l'Université Paris 1 Panthéon-Sorbonne.

Je soussigné(e), Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), et en cette qualité susceptible d'accéder à des données à caractère personnel, reconnais le caractère confidentiel de ces données.

Je m'engage par conséquent, en application des articles 34 et 35 de la loi "Informatique et Libertés" du 6 janvier 1978 modifiée, ainsi que des articles 32 à 35 du Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016, à prendre toutes les mesures nécessaires et conformes à l'état de l'art et aux règles internes dans le cadre de mes attributions, afin de garantir la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher leur divulgation à des personnes non expressément autorisées à recevoir ces informations.

Plus particulièrement, je m'engage à :
- Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- Ne divulguer ces données qu'aux personnes expressément autorisées à les recevoir, en raison de leurs fonctions, qu'elles soient des personnes physiques ou morales, publiques ou privées ;
- M'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- Ne procéder à aucune reproduction des données, sauf si cela est indispensable à l'accomplissement de mes missions ;
- Mettre en œuvre toutes les mesures appropriées, conformes aux standards de sécurité en vigueur, pour prévenir tout usage détourné, frauduleux ou non sécurisé de ces données, et assurer leur protection tant physique que logique.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, après la cessation de mes fonctions, quelle qu'en soit la cause et tant que les données n'auront pas été rendues publiques par la Société, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la règlementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du Code pénal.

Fait à _____ le _____ en _____ exemplaires.

Nom : _____

Signature : _____

ANNEXE 2 : Mention d'information à destination des personnes concernées

Informations sur le traitement et les droits relatifs à vos données personnelles dans le cadre du projet [nom du projet de recherche]

Dans le cadre de votre participation au projet de recherche [nom du projet de recherche], nous souhaitons vous informer sur la collecte et le traitement de vos données personnelles, ainsi que sur vos droits en matière de protection des données, conformément au Règlement Général sur la Protection des Données (RGPD).
Attachés à la transparence et à la protection de vos données tout au long de cette recherche, nous souhaitons nous assurer que vous comprenez bien leur utilisation. C'est pourquoi nous vous fournissons ces informations afin que vous soyez pleinement informé(e) des modalités de traitement de vos données et des moyens à votre disposition pour exercer vos droits.
À cet effet, vous trouverez ci-dessous les détails relatifs à la collecte, au traitement de vos données personnelles, ainsi que la procédure pour exercer vos droits :

Les informations recueillies seront traitées par [responsable de traitement]. La base légale du traitement est la mission d'intérêt public.

Les données collectées seront communiquées aux seuls destinataires suivants : [destinataires des données].

Elles sont conservées pendant [durée de conservation des données prévue par le responsable du traitement ou critères permettant de la déterminer].

Conformément au RGPD, vous disposez de plusieurs droits relatifs à vos données personnelles, que vous pouvez exercer à tout moment :
- Droit d'accès : Vous avez le droit de savoir quelles données vous concernant sont traitées et de demander une copie des informations en notre possession.
- Droit de rectification : Si vous constatez que des données vous concernant sont inexactes ou incomplètes, vous pouvez demander leur correction ou leur mise à jour.
- Droit à la limitation du traitement : Vous avez la possibilité de demander que nous limitions l'utilisation de vos données dans certaines situations, par exemple, si vous contestez leur exactitude ou si le traitement est jugé illégal mais que vous ne souhaitez pas effacer vos données.
- Droit d'opposition : Vous avez le droit de vous opposer, pour des raisons tenant à votre situation particulière, au traitement de vos données personnelles.

Toutefois, une fois la phase d'analyse des données engagée, l'exercice de certains de ces droits pourrait être restreint afin de ne pas compromettre la validité scientifique, l'intégrité ou les résultats de la recherche.

Consultez le site cnil.fr pour plus d'informations sur vos droits.

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans le cadre de ce dispositif, vous pouvez contacter [responsable de traitement + ses coordonnées mail] ou le cas échéant, notre délégué à la protection des données : dpo@univ-paris1.fr

Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

Si vous rencontrez des difficultés à compléter les champs entre crochets, référez-vous aux fiches explicatives associées : Responsable de traitement (fiche 1), Base légale (fiche 2), Destinataires des données (fiche 6), durée de conservation (fiche 10).