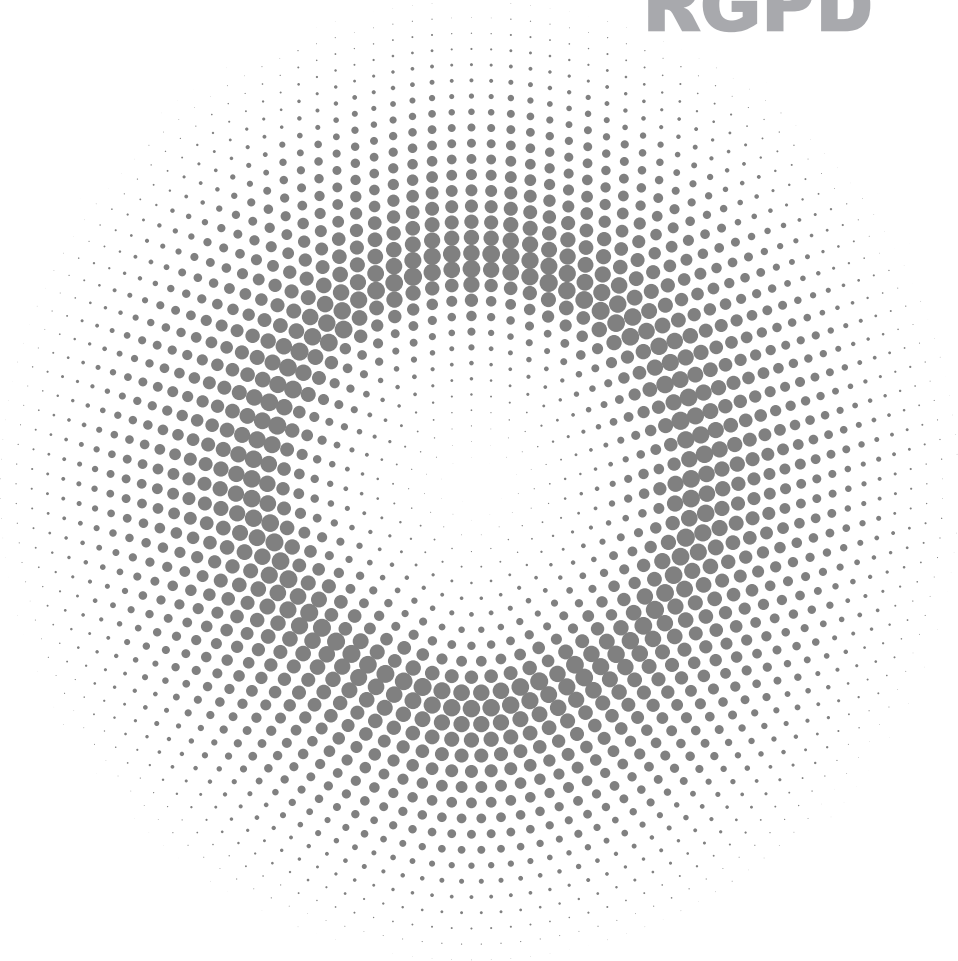
# Règlement général pour la protection des données

# RGPD



## Fiches pratiques à destination des chercheurs

Edition : Direction de la recherche et des études doctorales / université Paris Nanterre

**Réalisation des fiches pratiques :**

Catherine Delplanque, Nawale Lamrini, Fabrice Leclère, Lionel Maurel

**Avec le concours de :**

Isabelle Autran, Nabil Belkouch, Jose-Manuel Coelho, Claire Hanen, Julie Nordin

## Sommaire

# Qui est propriétaire des données ?

La plupart des conventions d'attribution de financement ou de partenariat insistent sur la question de la « **propriété des résultats de recherche** ». Néanmoins, la notion de propriété est à manier avec précaution en ce qui concerne les données.

Les chercheurs sont certes propriétaires d'un **droit d'auteur** sur les œuvres qu'ils produisent dans le cadre de leurs activités (textes d'articles ou d'ouvrages, photographies, cours, interventions, etc.). Néanmoins, les données relèvent d'un autre régime, lié au droit des bases de données.

Dans ce cas, le droit de propriété appartient légalement au « **producteur » de la base de données**, compris au sens de la personne qui réalise l'investissement financier et matériel nécessaire à la constitution de la base. Il s'agira donc en général de **l'établissement de tutelle** des chercheurs qui sera considéré comme le titulaire effectif du droit de propriété.

Néanmoins depuis l'adoption de la loi République numérique, les établissements d'enseignement supérieur et de recherche sont soumis – au même titre que les autres administrations – à une obligation d'ouverture des données qu'ils produisent. Cela signifie qu'ils sont tenus de diffuser en ligne et de rendre librement et gratuitement réutilisables ces informations (**principe d'ouverture ou d'Open Data par défaut**). Il en résulte que si les droits de propriété des universités sur les données de recherche existent formellement, ils ne peuvent plus être opposés aux droits des réutilisateurs.

Il convient cependant de noter que l'obligation d'ouverture ne vaut pas lorsque des données de recherche contiennent des **données à caractère personnel** afin de protéger la vie privée des individus concernés (voir fiche sur la définition des données personnelles).

Sur les données personnelles les concernant, les individus ne sont pas considérés non plus comme disposant d'un droit de propriété au sens propre du terme. La législation protège en effet les données en tant qu'**attributs des personnes** en leur reconnaissant des droits fondamentaux destinés à leur permettre d'en contrôler l'usage.

Au final, il est assez trompeur d'utiliser la notion de propriété pour comprendre exactement les règles liées aux données (et plus encore aux données à caractère personnel).

## Est-ce que je manipule des données personnelles ?

Par données personnelles, on entend « **toute information permettant d'identifier une personne directement ou indirectement** ». Contrairement à une idée reçue, il ne s'agit donc pas uniquement de données « confidentielles » ou relative à la vie privée des individus, mais bien toute information ayant un pouvoir d'identification.

Le nom et le prénom sont les données à caractère personnel les plus évidentes. Mais on range aussi dans cette catégorie de nombreux éléments dont voici **quelques exemples indicatifs** :

- Tous les identifiants d'une personne (adresse physique ou IP, adresse mail, numéro de téléphone, numéro de sécurité sociale, numéro de compte en banque, etc.)
- Ses caractéristiques physiques (taille, poids, couleur des yeux et des cheveux, état de santé, ADN, empreintes digitales ou rétiniennes, image, son de la voix, etc.)
- Ses opinions et comportements (idées politiques, convictions religieuses, appartenances associatives, orientation sexuelle, habitudes de consommation, goûts, etc.)
- Les données d'usage, type géolocalisation, l'image, historique de navigation ou d'achats, contenus postés, etc.

Des jeux de données ne contenant pas le nom des personnes peuvent encore être considérés comme des informations à caractère personnel s'ils permettent leur identification. Un jeu peut ne pas être identifiant en lui-même, mais aussi le devenir indirectement par croisement avec d'autres données.

Pour prendre un exemple, un jeu de données peut comporter uniquement le lieu de résidence et la profession, sans mentionner le nom. Mais si une personne est la seule à exercer sa profession dans sa localité, la réidentification indirecte sera aidée et les données seront considérées comme ayant un caractère personnel.

**Qui est le « responsable du traitement » ?**

La réglementation relative à la protection des données s'applique dès qu'il y a « **traitement » des informations personnelles**, avec une définition très large incluant toute forme de collecte, enregistrement, conservation, consultation, diffusion, interconnexion, enrichissement, etc.

Un chercheur qui réalise de telles opérations est considéré comme un « responsable de traitement » au sens de la législation du moment qu'il détermine les finalités et les modalités du traitement (le but du projet de recherche et les moyens mis en œuvre pour l'atteindre).

La qualité de responsable de traitement impose le respect de nombreuses obligations et elle oblige à assumer **plusieurs types de responsabilité** (civile, pénale) en cas de violation de la réglementation et de dommages causés.

Dans le cadre d'un projet de recherche la personne responsable de traitement est le chercheur, ou s'il est membre d'une UMR son directeur ou sa directrice d'unité. Mais les risques pèsent aussi sur ses autorités de tutelle, qui verront leur responsabilité juridique engagée (voir la fiche sur les risques).

Il existe des cas de **co-responsabilité**, lorsque plusieurs entités déterminent conjointement les finalités d'un traitement ou en cas de prestations de traitement confiées à un tiers.

## Les données de mon projet sont-elles sensibles ?

Le RGPD considère comme **sensibles** « les informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle » des personnes. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes, mais les chercheurs bénéficient de certaines dérogations en cas de traitement de telles informations (voir la fiche sur les droits des personnes).

Néanmoins, alors que les formalités préalables ont été globalement supprimées par le RGPD, il reste généralement nécessaire de solliciter un **avis de la CNIL** pour traiter des données sensibles. Lorsque le traitement des données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, la réalisation d'une analyse d'impact sur la protection des données (PIA) est demandée.

**Le cas particulier des données de santé**

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

Les données de santé sont des données à caractère personnel particulières, faisant l'objet d'une **protection renforcée** dans les textes (règlement européen sur la protection des données personnelles, loi Informatique et Libertés, code de la santé publique, etc.) afin de garantir le respect de la vie privée des personnes.

La CNIL a adopté des nouvelles méthodologies de référence. Les recherches menées au sein de la ComUE Université Paris Lumières sont principalement concernées par les méthodologies MR-001 MR-003, MR-004, qui offrent un cadre sécurisé pour la mise en œuvre des traitements de recherche dans le domaine de la santé.

Ces référentiels encadrent les traitements de données de santé à des fins de recherche. Si le traitement est conforme à l'une de ces méthodologies, la demande d'autorisation n'est pas nécessaire.

Dans tous les cas, il est conseillé de contacter votre DPD (voir fiche « quelles formalités accomplir et quel est le rôle du DPD ») pour être guidé dans les démarches à réaliser.

## Quelles sont les modalités de collecte des données et leurs implications ?

La collecte de données à caractère personnel peut s'opérer de deux manières différentes : soit **directement** auprès des personnes concernées, soit **indirectement** en passant par un tiers détenant des données.

La **collecte directe** de données auprès des personnes peut prendre diverses formes : questionnaires ou formulaires à remplir, enquêtes, entretiens, notamment sur des supports audio et vidéo, etc. Dans une telle situation, il est nécessaire de recueillir par écrit le **consentement libre, éclairé, spécifique et explicite** des personnes, en leur indiquant notamment la finalité pour laquelle les données sont collectées. Pour offrir une sécurité maximale, un tel consentement devrait être systématiquement être **recueilli par écrit** au moyen de formulaires normalisés qui devront être conservés pour servir de preuve.

Les chercheurs bénéficient en outre de la faculté de **collecter indirectement** des données personnelles en se les faisant remettre par un tiers détenteur (association, administration, entreprise). Ce tiers doit avoir en premier lieu collecté légalement ces données pour des finalités qui lui sont propres. La remise des données à des chercheurs réalise alors un changement de finalité jugé compatible par la législation. Ce type de collecte indirecte de données ne dispense pas les chercheurs de respecter les **droits des personnes**.

Dans tous les cas, la collecte des données doit se limiter à ce qui est strictement nécessaire pour atteindre la finalité recherchée. C'est le **principe de minimisation** imposant que les données à caractère personnel recueillies doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

On ne peut de ce fait collecter des données personnelles en vue de les accumuler sans objectif précis et déterminé à l'avance, ni modifier substantiellement la finalité d'un traitement sans revenir auprès des personnes concernées afin d'obtenir à nouveau leur consentement.



## Que faire pour respecter les droits des personnes ?

La législation reconnaît aux personnes une série de droits sur les données les concernant qu'elles peuvent activer et que les responsables de traitement doivent être en mesure de respecter :

- **Droit à l'information** : toute personne doit être prévenue que des données la concernant sont traitées et informée notamment des finalités poursuivies.
- **Droits d'accès et de rectification** : toute personne peut demander à un responsable de traitement la communication des données la concernant et exiger leur modification en cas d'erreur.
- **Droits d'opposition et à l'effacement** : toute personne ayant consenti à un traitement de données peut à tout moment retirer ce consentement pour faire cesser le traitement et demander à ce que les informations la concernant soient détruites (droit à l'oubli).
- **Droit à la portabilité des données** : toute personne peut demander à un responsable de traitement que lui soit remise les données la concernant dans un format interopérable afin qu'elle puisse les réutiliser.

Un responsable de traitement doit informer par des mentions adéquates les personnes de l'existence de ces droits et se tenir prêt à satisfaire les demandes portées à sa connaissance par les individus dans un délai d'**un mois**.

Les chercheurs bénéficient de **certaines dérogations** limitées opposables à ces droits. Ils peuvent par exemple s'abstenir d'informer les personnes avant un traitement, si « cet acte d'information s'avère impossible à réaliser ou exige des efforts disproportionnés ». Ils peuvent également refuser de faire droit à des demandes d'accès, d'opposition ou d'effacement si leur satisfaction compromettrait la poursuite de l'objectif de recherche.

Ces dérogations sont néanmoins à manier avec précaution, car elles ne peuvent être invoquées qu'en **cas de stricte nécessité** lorsque l'exercice des droits des personnes serait susceptible de rendre impossible la recherche visée. Il faut donc être en mesure de justifier au cas par cas un refus opposé à une personne cherchant à faire valoir ses droits, en fonction du contexte particulier de chaque recherche.

## Quelles formalités accomplir et quel est le rôle du délégué à la protection des données (DPD ou DPO) ?

La législation antérieure au RGPD imposait un régime de déclaration (et parfois d'autorisation) préalable en cas de traitement de données à caractère personnel à effectuer auprès de la CNIL. Le RGPD prévoit un allègement des obligations en matière de formalités préalables, qui sont remplacées par des mesures visant à **responsabiliser directement les acteurs**.

En contrepartie de la suppression de certaines formalités, le responsable de traitement doit désormais être en mesure de démontrer, à tout moment, sa conformité aux exigences du RGPD en traçant toutes les démarches nécessaires (*principe d'accountability*).

Cela se traduit notamment par l'obligation d'inscrire les traitements dans un registre qui doit être tenu par le responsable de traitement, en faisant figurer les informations suivantes :

- **les parties prenantes** (responsable de traitement, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
- **les catégories de données traitées** (personnelles, sensibles, de santé, etc.) ;
- **à quoi servent ces données** (ce que vous en faites), **qui accède aux données** et **à qui elles sont communiquées** ;
- **combien de temps** vous les conservez ;
- **comment** elles sont **sécurisées** ;
- **comment** est organisé le respect **du droit des personnes.**

La tenue du registre est une obligation pour chaque responsable de traitement et donc par les chercheurs effectuant des recherches impliquant des données à caractère personnel. La tenue du registre peut s'effectuer de différentes manières au sein des établissements (un seul registre centralisé ou des registres par service).

Le RGPD impose aux établissements la désignation d'un DPD/DPO (Délégué à la Protection des Données/Data Protection Officer) prenant la suite des CIL (Correspondants Informatique et Libertés).

Le Délégué à la Protection des Données, chargé de la conformité en matière de protection des données au sein de son organisme, s'occupe principalement :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle (CNIL) et d'être le point de contact de celle-ci.

## Est-ce que je peux/dois anonymiser les données ?

Le RGPD ne s'applique qu'aux informations susceptibles d'identifier des personnes. Si les données sont anonymisées, le RGPD ne s'applique pas. Le choix d'opérer ou non une anonymisation implique donc une réflexion rigoureuse selon le type de recherche et la sensibilité des données concernées.

**En cas de traitement de données sensibles, le choix de l'anonymisation permet d'éviter les formalités de la CNIL**. L'anonymisation peut être déterminée au départ par le chercheur pour des raisons juridiques et éthiques, scientifiques ou méthodologiques, mais l'anonymat peut également être un choix de l'informateur, soit pour des raisons de confidentialité, de protection de sa vie privée ou publique, soit pour des raisons juridiques ou de sécurité pour lui ou pour ses proches.

**Comment choisir les techniques d'anonymisation ?**

Plusieurs techniques d'anonymisation existent s'appuyant sur deux grands principes : transformer les données pour qu'elles ne se réfèrent plus à une personne déterminée ou généraliser les données de façon qu'elles ne soient plus spécifiques à un individu, mais communes à un ensemble de personnes.

Il existe différentes méthodes d'anonymisation basées sur des procédés plus ou moins complexes. Certaines s'appuient sur l'appauvrissement des données, d'autres sur l'effacement pur et simple d'une information, d'autres encore sur un traitement par un algorithme (hachage). Chaque technique présente des forces et des faiblesses au regard du risque de ré-identification.

L'anonymisation et la ré-identification de données sont des thématiques de recherche particulièrement actives et par conséquent il est indispensable, pour tout responsable de traitement mettant en œuvre des solutions d'anonymisation, d'effectuer une veille régulière pour préserver, dans le temps, le caractère anonyme des données produites.



**Un exemple d'outil d'anonymisation mis à disposition des chercheurs**

La Commission européenne dans le cadre du programme H2020 propose aux chercheurs l'outil Amnesia, une solution applicable à des données recueillies à l'état brut permettant une anonymisation des résultats.

https://amnesia.openaire.eu/

**Trois critères** permettent d'évaluer l'efficacité d'une solution d'anonymisation :

- **L'individualisation** : est-il toujours possible d'isoler un individu ?
- **La corrélation** : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- **L'inférence** : peut-on déduire de l'information sur un individu ?

Ainsi :

- un ensemble de données pour lequel il n'est possible ni d'individualiser ni de corréler ni d'inférer est a priori anonyme ;
- un ensemble de données pour lequel au moins un des trois critères n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de ré-identification.

## Quels réflexes pour la sécurisation des données ?

Le RGPD impose une **obligation de sécurisation des données** et toute fuite ou atteinte à l'intégrité des systèmes engage la responsabilité du responsable de traitement, avec des sanctions potentielles à la clé. En cas de **violation des données**, le **DPD doit être informé en premier lieu** pour aider aux démarches obligatoires vis-à-vis de la CNIL. Lorsque les fuites comportent des risques pour les personnes, il peut être nécessaire d'informer nominativement les personnes concernées. Outre les cas de piratage, le simple fait de perdre un ordinateur ou une clé USB contenant des données personnelles constitue un manquement à l'obligation de sécurisation.

Il importe dès lors d'adopter de bonnes pratiques en matière de sécurité informatique pour l'ensemble des postes de travail et de collecte (ordinateurs, smartphones, tablettes, etc.).

### Protection contre le vol et chiffrement

**Prévoir des mécanismes de protection contre le vol** (par ex. câble de sécurité, marquage visible du matériel) et de limitation de ses impacts (par exemple, verrouillage automatique, chiffrement).

Prévoir un mécanisme de **verrouillage automatique** de session en cas de non-utilisation du poste pendant un temps donné, et de même, sur les smartphones et tablettes, en plus du code PIN de la carte SIM, activer le verrouillage automatique du terminal et exiger un code secret pour le déverrouiller (mot de passe, schéma, etc.).

**Prévoir aussi la purge des données collectées sur les supports mobiles** sitôt qu'elles ont été transférées au système d'information de l'organisme.

**Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles** (ordinateurs portables, smartphones tablettes, clés USB, disques durs externes, CD-R, DVD-RW, etc.) en chiffrant soit le support/disque dans sa totalité, ou seulement les fichiers/dossiers concernés.



Pour transmettre des pièces: **chiffrer les pièces** sensibles à transmettre, si cette transmission utilise la messagerie électronique ou avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur portable).

Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers (utilisant **SSL/TLS**, comme https, ftps), en utilisant les versions les plus récentes des protocoles.

**Assurer la confidentialité des codes 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).

**Ce qu'il ne faut pas faire**

Transmettre des fichiers contenant des données personnelles en clair via des messageries grand public.

## Stockage des données

**Mettre en œuvre des mécanismes maîtrisés de sauvegarde ou de synchronisation** des postes nomades, pour se prémunir contre la disparition des données stockées.

**Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme** plutôt que sur les postes de travail (contacter votre DSI pour des informations sur les éléments mis en place dans votre établissement).

**Utiliser des supports externes permettant un chiffrement matériel** : exemple clé USB avec code de 7 à 15 chiffres.

Limiter la connexion d'autres supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable.

**Ce qu'il ne faut pas faire**

Utiliser comme outil de sauvegarde ou de synchronisation les services cloud installés par défaut sur un appareil sans analyse approfondie de leurs conditions d'utilisation et des engagements de sécurité pris par les fournisseurs de ces services. Voir avec le DPD les mentions légales.



## Accès aux données

**Limiter le stockage des données sur les postes** nomades au strict nécessaire, et éventuellement l'interdire lors d'un déplacement à l'étranger

Des **niveaux d'habilitation** différenciés doivent être mis en place en fonction des besoins pour les personnes ayant accès aux données.

**Ce qu'il ne faut pas faire**

- Créer ou utiliser des comptes partagés par plusieurs personnes.
- Donner des droits d'administrateur à des utilisateurs n'en ayant pas besoin.
- Accorder à un utilisateur plus de privilèges d'accès ou d'usage que nécessaire.
- Oublier de retirer des autorisations temporaires accordées à un utilisateur (pour un remplacement, par exemple).

## Les données peuvent-elles voyager au-delà des frontières ?

Le RGPD a un effet direct dans toute l'Union Européenne et il va harmoniser les règles de protection dans tous les Etats-Membres. L'un de ses objectifs et de favoriser la circulation des données à l'intérieur de l'Union et l**e transfert de données entre pays européens** est donc possible (sous réserve de respecter toutes les autres conditions posées par le règlement).

Pour les **transferts de données en dehors de l'Union Européenne**, il est nécessaire de prendre en compte la distinction établie par la CNIL entre les « pays adéquats » (garantissant un niveau de protection comparable à celui de l'Union) et les pays non adéquats, dont la liste figure sur le site de la CNIL.

Le transfert de données hors de l'Union européenne (UE) et de l'Espace Economique Européen (EEE) reste néanmoins possible, y compris vers un pays non adéquat, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent alors être encadrés en utilisant différents outils juridiques.

**Ainsi, par exemple, pour un projet de recherche en Colombie, qui n'est pas un pays adéquat, le projet de recherche devra intégrer la protection des données personnelles, s'il y en a, et ce dès l'origine, par différents mécanismes possibles, notamment par voie de convention entre les partenaires impliqués. Ce qui suppose une anticipation et un dialogue avec les différents intervenants et partenaires institutionnels.**

Pour les entreprises du secteur privé, les BCR (*Binding Corporate Rules* ou règles d'entreprises contraignantes) sont utilisables. S'agissant du secteur public, d'autres modes de transferts sont possibles en fonction des situations.

Le RGPD élargit la gamme d'outils juridique permettant d'encadrer les transferts. Ils pourront être utilisés tant par les responsables de traitement que par les sous-traitants.



## Comment procéder pour l'archivage des données ?

En principe, des données personnelles ne peuvent être conservées au-delà de ce qui est nécessaire pour atteindre la finalité du traitement envisagé et **doivent être détruites** au terme d'un délai prévu à l'avance et indiqué dans le registre de traitement. D'après le RGPD, la durée de conservation doit être limitée « au strict minimum ».

Néanmoins, le texte prévoit **une dérogation pour les traitements réalisés à des fins de recherche** : les données peuvent en effet être conservées au-delà de la durée du projet de recherche initial indiquée au registre.

Mais la conservation au-delà de la durée du projet initial doit suivre alors **une procédure d'archivage définitif** des données impliquant leur remise à un service disposant de la compétence légale pour procéder à cette opération. Dans le cas des universités, ce sont normalement les services d'Archives départementales qui sont compétentes, mais ils peuvent déléguer aux services des archives des universités la possibilité de recueillir certains documents, y compris des données.

Une fois les données de recherche ayant fait l'objet d'une procédure définitive, leur communication suit les règles liées à la consultation des archives, ce qui peut impliquer le respect des délais de communicabilité ne pouvant être levés que par voie de dérogation afin de protéger la vie privée des personnes.

Dans tous les cas, contacter votre DPD et/ou le service des archives de votre établissement pour connaître la procédure à suivre.

## Qui est responsable des traitements en cas de projet de recherche collaboratif ?

Lorsqu'**un projet de recherche implique plusieurs partenaires**, il convient d'utiliser la **voie contractuelle** pour formaliser les obligations et les droits de chaque partie en matière de protection des données. Le type de contrat le plus fréquemment employé est le contrat de collaboration de recherche ou convention de collaboration de recherche.

Pour établir la répartition des responsabilités entre les différents partenaires, il est possible de suivre cette règle : seront considérés comme co-responsables du traitement les parties **co-propriétaires de droits de propriété intellectuelle** sur les résultats de la recherche. Il n'est ainsi pas possible de revendiquer une propriété sans assumer les responsabilités qui en découlent.

La répartition des droits de propriété intellectuelle en cas de projet de recherche collaborative peut s'opérer de différentes manières. Des partenaires fournissant des apports similaires produiront des « **œuvres de collaboration** » et devront alors partager la qualité de « responsables conjoints du traitement » des données personnelles.

Lorsqu'un des partenaires joue un rôle plus directeur par rapport aux autres, il est possible que le résultat constitue une « œuvre collective » définie juridiquement comme « *l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé*. » Dans ce cas, on pourra désigner contractuellement un « chef de file » responsable du traitement dans le cadre d'une recherche collaborative avec des parties apportant leur concours uniquement.



Dans tous les cas, au sens de la protection des données personnelles, il est possible de manière contractuelle d'établir une corrélation entre la Donnée et la Propriété Intellectuelle. Tout passera par la voie contractuelle et il convient de rédiger les articles concernant les dispositions relatives à la protection des données au sens de la co-responsabilité.

**Les « responsables conjoints de traitement » et leurs obligations**

Le RGPD prévoit que « lorsque deux responsables de traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. »

Ils sont alors tenus d'adopter une convention définissant leurs obligations respectives pour assurer le respect des exigences liées à la protection des données personnelles, notamment la manière dont ils s'organisent pour permettre l'exercice des droits des personnes (voir fiche sur les droits des personnes).

## Quels sont les risques encourus pour moi, mon projet, mon institution ?

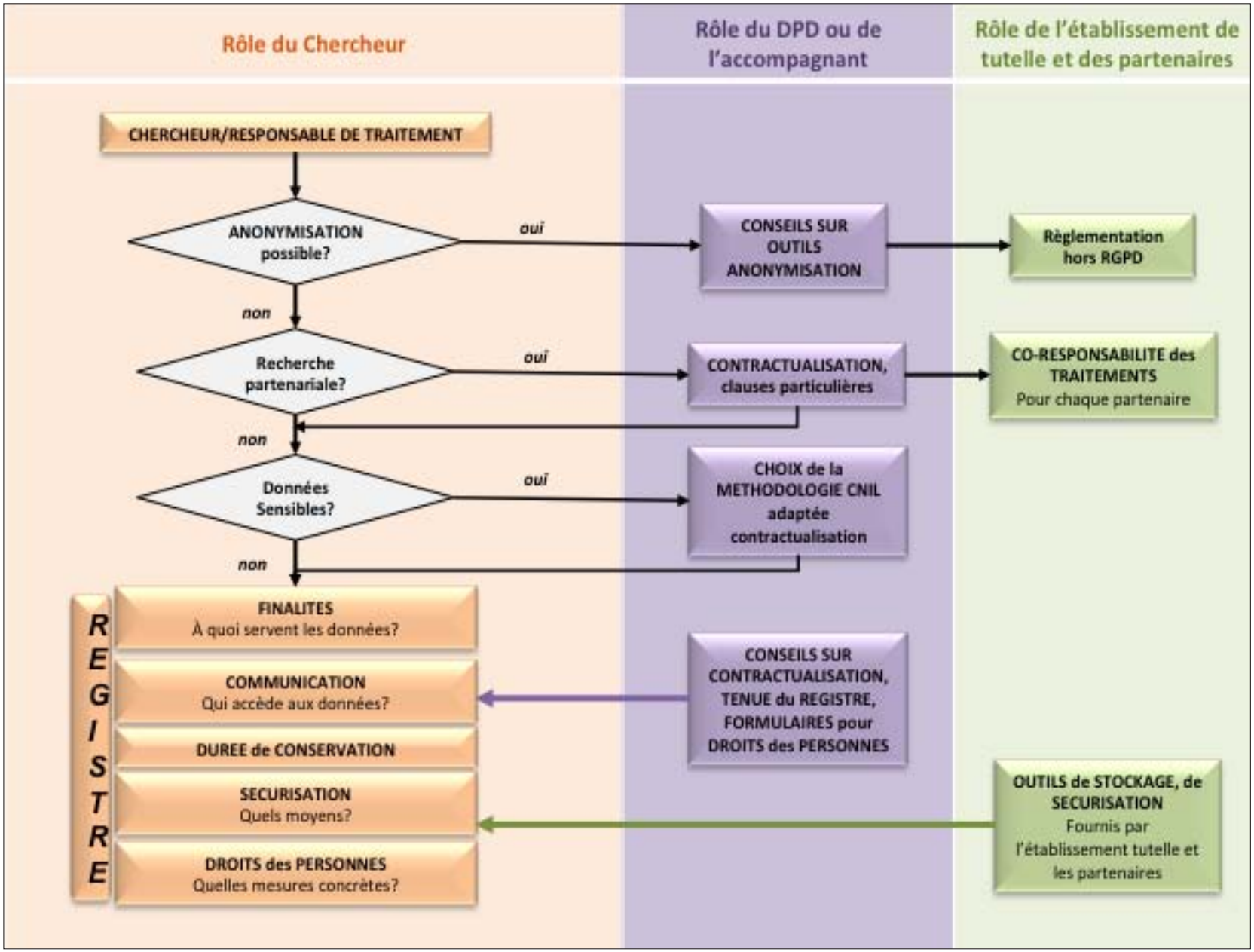
Les risques encourus en cas de non-respect de leurs obligations par les divers intervenants sont de plusieurs ordres (juridiques, financiers, de réputation, etc.)

- **Atteinte à l'image** et à la réputation des établissements.
- **Sanctions pénales** : amendes pénales jusqu'à 300 000 € et peine d'emprisonnement jusqu'à 5 ans.
- **Responsabilité civile** des établissements en cas de dommages causés du fait de la violation des données personnelles.
- **Frais de notification** de la violation des données personnelles à la CNIL, voire aux personnes concernées.
- **Amende administrative** en cas d'action de la CNIL ou d'une autorité administrative. Le risque d'une sanction financière peut aller jusqu'à 4 % du chiffre d'affaires annuel global (secteur privé), ou 20 millions d'euros (secteur public).

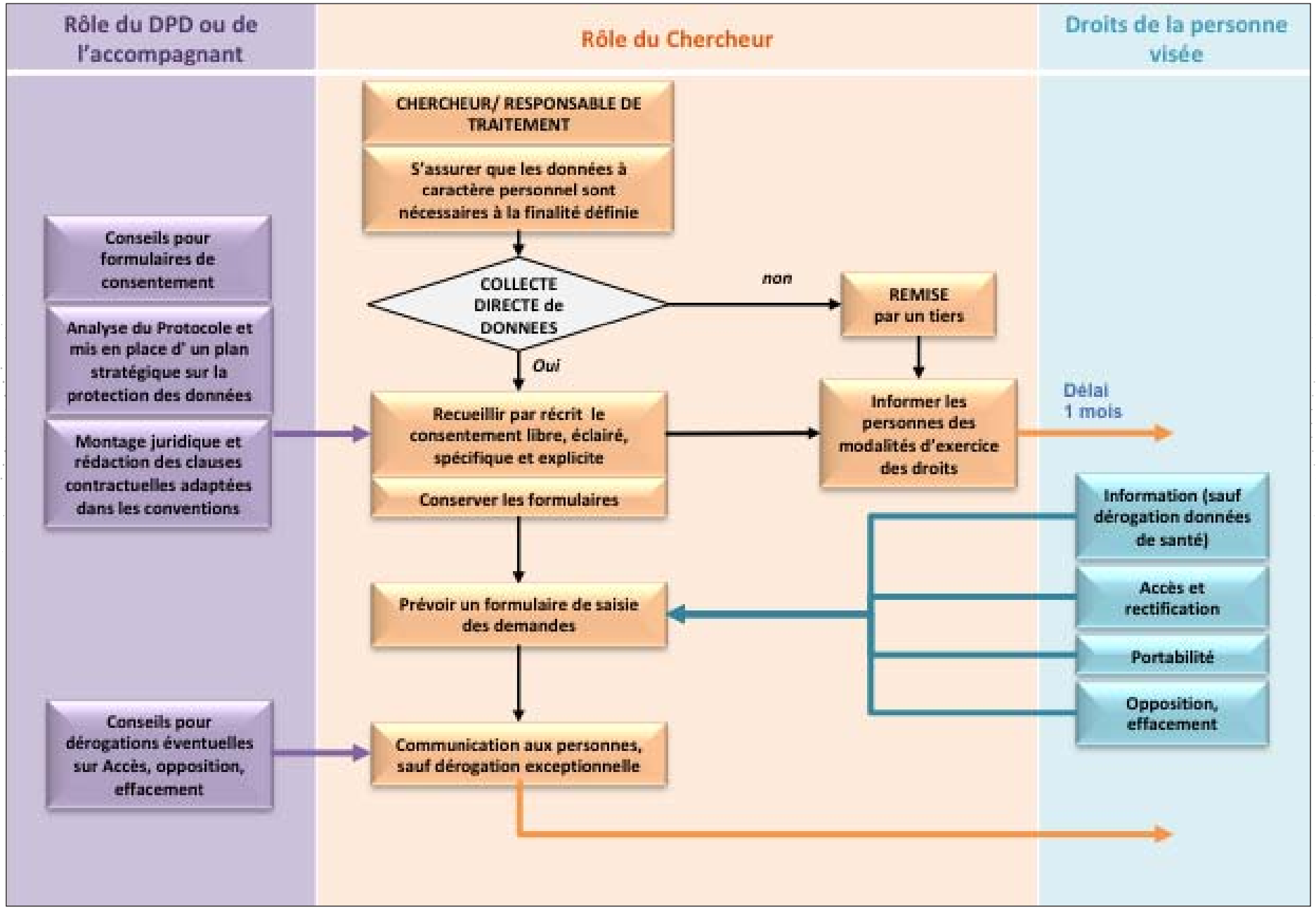
Il s'agit alors :

- **de prendre en compte la protection des données personnelles dès la conception du projet de recherche** (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données). Pour cela, appuyez-vous sur les conseils du délégué à la protection des données ;
- d**e sensibiliser et d'organiser la remontée d'information** en informant et formant vos collaborateurs ;
- d**e traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits** (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen) ;
- **d'anticiper les violations de données** en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

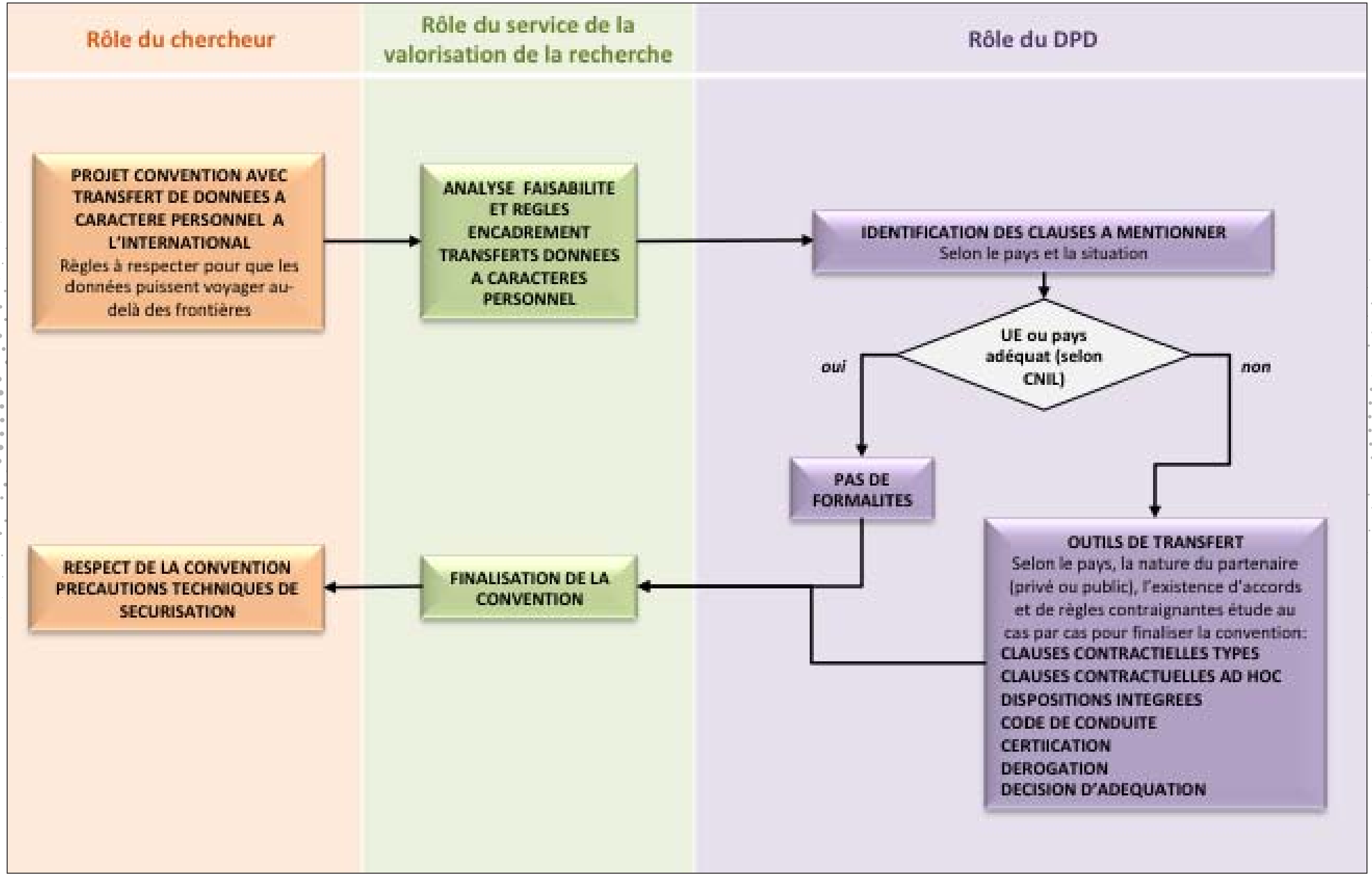
# Données personnelles - démarches



# Données personnelles - droits des personnes



# Données personnelles - transfert à l'étranger



# Glossaire et liens utiles

**Accountability**

Ce terme désigne l'obligation pour les organisations de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

**Chiffrement**

Le chiffrement est un procédé qui consiste à transformer une donnée qui peut être lue par n'importe qui en une donnée qui ne peut être lue que par son créateur et son destinataire.

**Clauses Contractuelles Types**

Il s'agit de modèles de clauses contractuelles adoptées par la Commission européenne qui permettent d'encadrer les transferts de données personnelles hors de l'Union européenne.

**CNIL**

Commission Nationale Informatique et Libertés instituée par la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

**Donnée personnelle**

Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

**Données sensibles**

Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes

**DPD** ou **DPO**

Délégué à la protection des données, DPO pour *Data Protection Officer* en anglais.

**Fichier**

Un fichier est un traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés.



**Formalités préalables**

Ensemble des formalités déclaratives à effectuer auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles ; selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation.

**Habilitation**

Autorisation pour l'accès à un ensemble de données.

**Minimisation des données**

Le traitement doit porter sur les données personnelles strictement nécessaires afin d'atteindre la finalité du traitement.

**Open data**

L'open data désigne un mouvement, né en Grande-Bretagne et aux États-Unis, d'ouverture et de mise à disposition des données produites et collectées par les services publics (administrations, collectivités locales...).

**PIA** (*Privacy impact assessment*) ou **AIPD** (Analyse d'impact relative à la protection des données)

Le RGPD prévoit la mise en œuvre d'un PIA lorsqu'un traitement de données personnelles est susceptible de créer un risque élevé pour les droits et libertés des personnes. Il est obligatoire dans certains cas identifiés par la CNIL, et pour d'autres s'apprécie en fonction de critères précis. Le PIA est élaboré avec le DPD qui en contrôle l'exécution.

**Protocole**

Règles d'échange de données entre machines. Certains protocoles comprenant le chiffrement des données sont recommandés pour les données personnelles, comme SSL, https.

**RGPD**

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

**Responsable de traitement**

Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique,

le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

### Traitement de données à caractère personnel

Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction...).

### Transfert de données

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.



## Références numériques

CNIL : https://www.cnil.fr/fr
https://www.cnil.fr/fr/glossaire

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

Règlement européen sur la protection des données :
https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique : https://tinyurl.com/ycagwmdo

## Contacts

Université Paris Nanterre

dpo@liste.parisnanterre.fr
Service des Affaires Juridiques et Institutionnelles (SAJI)
Direction de la Recherche et des Etudes Doctorales (DRED)

UNIVERSITÉ PARIS 8 VINCENNES SAINT-DENIS

cil@univ-paris8.fr, fleclere@univ-paris8.fr
01 49 40 67 75
Direction Générale des Services

cnrs

Pour les chercheurs CNRS, prendre contact avec votre UMR

# Règlement général pour la protection des données

Edition 2019 **RGPD**