Projet de recherche en SHS et données personnelles : comment respecter le RGPD ?

Rebecca ROUSSEAU, adjointe DPO et RSSI
En charge de l'ensemble du volet recherche
DSIUN-CCP : Cellule cybersécurité et protection des données
rebecca.rousseau@univ-paris1.fr

PANTHÉON SORBONNE
UNIVERSITÉ PARIS 1

Tour de table

- Quel est votre établissement et quel type de recherche y menez-vous (thèse, post-doc, etc.) ?

- Quel est le sujet de votre projet de recherche ?

- Qu'attendez-vous de cette formation (objectifs d'apprentissage) ?

- Quel est votre niveau de connaissance du RGPD ? (aucun, débutant, intermédiaire, avancé…)

Objectifs

- Comprendre ce qu'est le RGPD

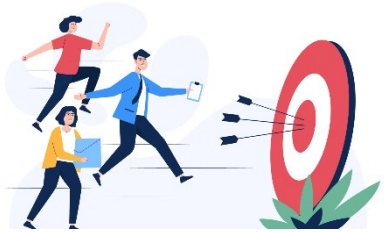
- Déterminer si vous êtes concerné(e)

- Mesurer les risques liés au non-respect du RGPD

- Prendre conscience de ses obligations et de sa responsabilité

- Assimiler les étapes essentielles de mise en conformité

- Réfléchir et mettre en œuvre les premières actions concrètes pour compléter sa déclaration de conformité RGPD à l’aide des ressources fournies



Programme de la formation

Partie 1 : Éléments introductifs au RGPD

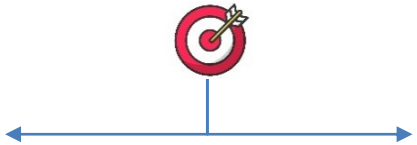
Partie 2 : S’assurer du respect du RGPD dans son projet

- Fiche 1* : Contexte et éléments généraux
- Fiche 2* : Les finalités du traitement de données
- Fiche 3* : Base légale de traitement
- Fiche 4* : Personnes concernées
- Fiche 5* : Données personnelles traitées
- Fiche 6* : Destinataires des données
- Fiche 7* : Gestion des demandes d’exercice de droit des personnes concernées
- Fiche 8* : Modalités d’information auprès des personnes concernés
- Fiche 9* : Stockage et hébergement des données
- Fiche 10* : Durée de conservation
- Fiche 11* : Sécurité des données
- Fiche 12 : Transferts des données hors de l’Union Européenne
- Fiche 13 : Sous-traitance
- Fiche 14 : Analyse d'impact relative à la protection des données

Éléments introductifs au RGPD

Qu’est-ce que le RGPD ?

Règlement **G**énéral sur la **P**rotection des **D**onnées



Renforcer le contrôle des individus sur l’utilisation faite de leurs données

Établir un cadre de gestion pour les responsables manipulant ces données (obligations légales)

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

OUI : RGPD applicable au domaine de la recherche scientifique

Manipulations données de recherche : données d’observation, d’expérimentation, de simulation, de référence…

Possible existence de données personnelles : mail, genre, âge…

⚠ SHS particulièrement exposées au RGPD car elles impliquent l’étude de la personne humaine

Quelle importance le RGPD a-t-il dans le cadre de mon projet de recherche ?

Gérer vos données de recherche de manière responsable, éthique et conforme

- Amélioration de la qualité de vos travaux
- Facilitation de la réutilisation et du partage des données (science ouverte)
- Prévention des risques juridiques
- **Renforcement de votre réputation et crédibilité** (confiance des participants)

- Attentes croissantes des organismes de financement (atout pour se démarquer dans les candidatures)
- Demandes de preuves de conformité RGPD lors de l'établissement de conventions de recherche (ex. DARES), lors de publication auprès d'éditeurs…

Perte des avantages liés à la conformité ci-contre

- Engagement de votre responsabilité civile en cas de préjudice
- Sanctions administratives (CNIL) ou pénales pour l'établissement (jusqu'à 300 000 € d'amende et 5 ans de prison)

- Atteinte à l'éthique de la recherche scientifique
- Impact sur l'image de l'université
- Perte de confiance des partenaires et du public (**conséquences sur l'ensemble de la communauté universitaire**)

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

Principe *d'accountability* (responsabilité)

démarche pro-active

contactez votre DPO

Déclaration de conformité RGPD

Fiche ? Registre ?

Comment remplir une fiche dans le registre de traitement ?

- Quoi ? Formulaire en ligne comportant de différents champs / questions (une trentaine).
- Quand ? AVANT de commencer la collecte des données : « *privacy by design* »

Vous n'y connaissez rien en matière de RGPD ? Pas de panique !

Prenez contact avec votre Délégué à la Protection des Données (DPO) afin d'initier votre mise en conformité.

⚠ Le DPO ne complétera pas la fiche à votre place : il s'agit de votre déclaration !

QUIZ : Éléments introductifs au RGPD

Q1 : Pour prouver ma conformité au RGPD, je dois :  C'est à vous !

Déclarer la conformité de mon projet dans le registre des traitements de l'établissement en me rapprochant de mon Délégué à la protection des données (DPO).

Si je suis inscrit(e) en thèse dans une école doctorale de Paris 1

Mon DPO : dpo@univ-paris1.fr

Dans le cas où je serais chercheur accueilli au sein d'un laboratoire de recherche :

Si c'est une unité de recherche (UR) propre à Paris 1

dpo@univ-paris1.fr

Si c'est une unité mixte de recherche (UMR) partagées entre plusieurs tutelles

DPO variable * ⚠

** Se référer à la désignation officielle auprès de la CNIL et/ou à l'établissement de rattachement du directeur d'unité (DU)*

Fiche 1 : Contexte et éléments généraux

Quels sont les éléments généraux que je dois fournir ?

- Nom du projet de recherche

- Structure(s) et composante(s) : école doctorale, laboratoire de rattachement, partenariat(s)
- Un moyen de me contacter (mail institutionnel Paris 1)
- Responsabilité : Traitement en co-responsabilité ? Traitement en sous-traitance ?
- Déclaration CNIL antérieure
- Date de début du projet / date de fin prévisionnelle
- Documentations utiles (protocole, PGD…)

Fiche 2 : Les finalités du traitement de données

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

Il s’agit de l’objectif pour lequel vous collectez et utilisez ces données personnelles, autrement dit, la raison précise de leur traitement.
La finalité doit être déterminée, explicite et unique, afin de garantir que les données collectées ne soient pas réutilisées pour des objectifs différents de celui initialement prévu.

« *Si je collecte des données personnelles, c’est parce que j’en ai besoin pour…* »

Comment identifier mes finalités de recherche ?

- Quel est l'objectif de ma recherche ?
- Pourquoi ai-je besoin de collecter ces données personnelles en particulier ?
- En quoi ces données sont-elles essentielles à la réalisation de mon projet ?
- Quelles hypothèses ou questions de recherche vais-je explorer grâce à ces données ?

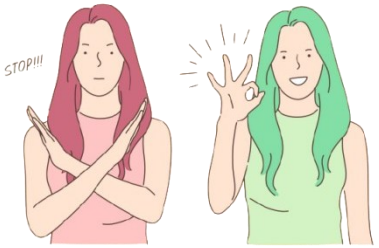
A vous ! Quelles sont vos finalités de recherche ?

Fiche 3 : Base légale de traitement

Qu’est-ce qu’une base légale ?

C’est le fondement juridique qui autorise et justifie le traitement des données personnelles, car cette démarche n’est pas autorisée en toutes circonstances.

Quelles bases légales utiliser dans le cadre de mon projet ?



- L'exécution d'une mission d'intérêt public : À privilégier dès lors que l’intérêt public du projet de recherche pourra être démontré.

- Le consentement de la personne concernée : Lorsque vous avez obtenu l’accord clair et explicite de la personne pour traiter ses données.

Que dois-je indiquer dans ma déclaration de conformité ?

- Précisez la manière dont votre projet contribue à la société et bénéficie au public.
- Indiquez comment le consentement des participants a été recueilli lors d’une collecte directe.

Fiche 4 : Personnes concernées

Qui sont les "personnes concernées » ?

Il s'agit des personnes dont les données personnelles sont collectées, traitées et utilisées. Autrement dit, celles qui fournissent leurs informations personnelles dans le cadre de vos recherches.

« *Mon champ d'étude porte sur les personnes…. »*

Comment identifier les personnes concernées ?

- Définissez l'objet de votre recherche : quel est son objectif et quelles données recherchez-vous ?
- Identifiez les sources de collecte des données.
- Déterminez les critères de sélection : précisez les caractéristiques des personnes incluses dans votre étude.

⚠ Précautions à prendre avec les personnes vulnérables : mineurs, majeurs protégés…

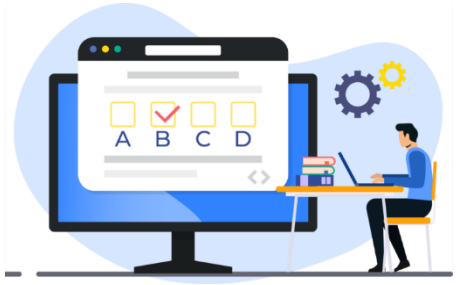
A vous ! Qui sont les personnes concernées dans vos travaux de recherche ?

Fiche 1 à 4

Q2 : Le RGPD me demande de détailler la « finalité de traitement » de mon projet. De quoi s'agit-il ?
La finalité de traitement désigne le but pour lequel les données personnelles sont collectées et utilisées.

Q3 : Le RGPD me demande de préciser la « base légale » applicable à mon projet ? De quoi s'agit-il ?
La base légale désigne la justification juridique (la légitimité) qui permet de traiter des données personnelles.

Q4 : Le RGPD me demande d'identifier les « personnes concernées » par mon projet. De qui s'agit-il ?
Les participants humains à mon projet de recherche, c'est-à-dire ceux qui fournissent des données personnelles.



Fiche 5 : Données personnelles traitées

Qu'est-ce qu'une donnée personnelle ? Mon projet est-il concerné ?

Information liée à une personne physique identifiée ou identifiable, permettant seule ou combinée à d'autres informations, d'identifier une personne.

Passez en revue les types de données que vous collectez : Sont-elles liées à des individus ? Peuvent-elles permettre de les identifier ou les rendre identifiable ?

Points de vigilance
- La notion de "donnée personnelle" est extrêmement large.
- Respect du principe de « minimisation des données ».

Que dois-je indiquer dans la fiche du registre des traitements ?

- Liste des catégories de données personnelles utilisées (attention aux données sensibles !)
- Méthode(s) de collecte de données personnelles utilisée(s)

A vous ! Quelles catégories de données personnelles traitez-vous et par quels moyens les collectez-vous ?

Fiche 6 : Destinataires des données

Qui sont les « destinataires » des données ?

Article 4 (RGPD) : « *La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel […]* »

Autrement dit, il s'agit de tous les partages de données collectées effectuées dans le cadre de vos recherches.
Ces destinataires peuvent être internes ou externes à votre projet.

Comment identifier les destinataires de mon traitement ?

- Qui pourra accéder aux données personnelles traitées dans le cadre de mon projet ?
- À qui vais-je partager ces données ?

Principe : limiter et encadrer les destinataires (signature d'un engagement de confidentialité – voir annexes du guide).

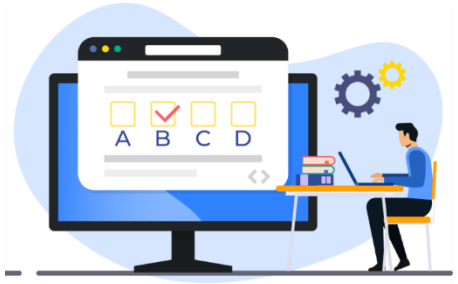
A vous ! Qui sont les destinataires de vos données personnelles ?

Fiche 5 et 6

Q5 : J’utilise une méthode de collecte indirecte de données, en réutilisant des données déjà préalablement collectées par un tiers, suis-je soumis au RGPD ?
OUI : L'application du RGPD est décorrélée de la méthode de collecte des données.

Q6 : Le RGPD me demande de respecter le principe de « minimisation des données ». De quoi s’agit-il ?
Le principe de minimisation des données consiste à ne collecter que les données personnelles strictement nécessaires au projet.

Q7 : Le RGPD me demande d’identifier les « destinataires » par mon projet. De qui s’agit-il ?
Les "destinataires" sont les personnes, organismes ou entités qui recevront ou pourront avoir accès aux données personnelles du projet.



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

Quels sont les droits des personnes concernées ?

L'application dans le domaine de la recherche

Les demandes d'exercice des droits sont généralement formulées dès les premières semaines suivant la collecte des données.

Des limitations à certains droits peuvent être admises, notamment en cas de risque de compromission majeure des objectifs ou des résultats de la recherche.

Comment traiter une demande d'exercice de droit ?

Accusez réception de la demande dès sa réception.

↓

Vérifiez systématiquement l'identité du demandeur.

↓

Traitez la demande et apportez une réponse dans un délai **d'un mois maximum** (prolongation possible).

Fiche 8 : Modalités d'information auprès des personnes concernés

Pourquoi informer les personnes concernées ?

Transparence

Demandes d'exercice de droit des personnes concernées

Quand et comment dois-je informer les personnes ?

Quand ? Avant la collecte / traitement des données personnelles (au plus tard un mois après en cas de collecte indirecte).

Comment ? L'information doit être facilement accessible !

Quelles informations dois-je obligatoirement fournir ?

- 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 / catégories de destinataires des données (fiche 6)
- Les droits des personnes concernées (fiche 8)
- La durée de conservation des données (fiche 10)

Pour vous aider, une mention détaillée est proposée en annexe du guide.

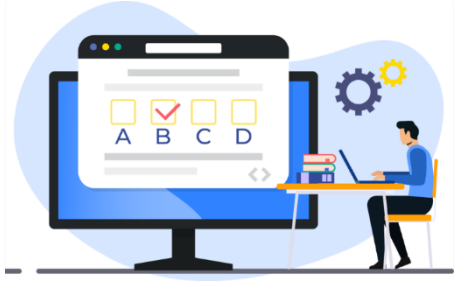
Fiche 7 et 8

Q8 : Combien de temps ais-je pour répondre légalement à une demande d'exercice de droit d'une personne concernées ?

1 mois qu'il est possible d'étendre à deux reprises (pour un total de 3 mois).

Q9 : Une mention d'information prouve-t-elle que la personne a donné son accord pour le traitement de ses données ?

NON : Il ne s'agit que de l'information visant à obtenir ce consentement qui doit être manifesté explicitement (preuve nécessaire).



Fiche 9 : Stockage et hébergement des données

A vous ! Quelles sont vos pratiques de stockage des données de votre projet ?

Où stocker et héberger vos données de recherche ?

- Plusieurs solutions existent, mais elles ne se valent pas toutes ! Privilégiez les plateformes institutionnelles ou les infrastructures disciplinaires.
- Exemple : l'infrastructure Huma-Num et son service d'hébergement collaboratif ShareDocs.

Huma-Num IR*

ShareDocs

Quelques recommandations à garder en tête ?

- Choisissez un support adapté à la sensibilité des données.
- Prenez en compte les besoins spécifiques de votre projet.
- Vérifiez où sont hébergées vos données.

Fiche 10 : Durée de conservation

Comprendre le cycle de vie des données ?

Recherche → **Archivage** → **Suppression**

Recherche	Archivage	Suppression
Données chaudes, modifications régulières	Réutilisation future ou réponse à des obligations légales	Suppression définitive ou anonymisation des données

Comment déterminer la durée de conservation de mes données ?

Le RGPD n'impose PAS de durée de conservation fixe : les données doivent être conservées uniquement le temps nécessaire à la réalisation de leur finalité. La durée peut être définie selon :

- Un événement certain (date précise fixée à l'avance).
- Un événement incertain (précisez les critères qui guideront l'effacement des données).

Adaptez la durée en fonction de la nature des données, leur utilité et leur sensibilité.
Besoin d'aide ? Consultez le Référentiel de gestion des archives de la recherche.

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

Anonymisation Suppression

Fiche 9 et 10

Q10 : Selon vous, pourquoi est-il essentiel de répertorier tous les supports où sont stockées mes données de recherche ?

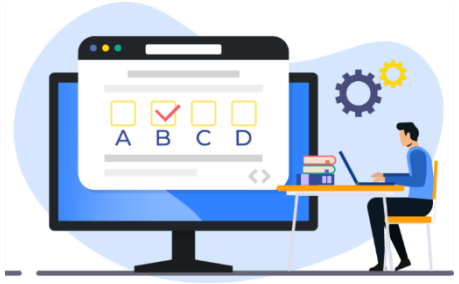
Faciliter la suppression complète des données : un bon inventaire permet d'éviter tout oubli et d'assurer un nettoyage efficace.

Q11 : Comment déterminer la durée de conservation de mes données ?

Fixer une date certaine lorsque possible ou, à défaut, définir des critères précis pour déterminer le moment de l'effacement.

Q12 : Que faire une fois la durée de conservation de mes données atteinte ?

Anonymisation et/ou suppression des données personnelles exclusivement.



Fiche 11 : Sécurité des données

Sécuriser les données : quels risques anticiper ?

Perte de disponibilité | Perte d'intégrité | Perte de confidentialité

Exemples ?

Mise en place de mesures de sécurité techniques et organisationnelles adaptées et proportionnées aux spécificités des projets.

Quelles mesures de sécurité technique ?

Gérer accès aux données

Authentifier les utilisateurs
Identifiants + MDP / MFA

Gérer les habilitations
compte individuel / principe du moindre privilège

Sécuriser les équipements

Protéger son poste de travail
MAJ de sécurité / antivirus / pare-feu / séparer les usages pro-perso

Protéger ses appareils nomades
Chiffrement / connexion sécurisée / transports en commun / départ à l'étranger

Conserver les données

Modalités de sauvegarde
Règle du 3-2-1 / utiliser des supports de stockage adaptées

Garantir la confidentialité
Chiffrement des données / sécurité physiques

Superviser diffusion données

Sécuriser les échanges
Chiffrement / canal sécurisé / FILEX / filigrane

Encadrer le partage-publication
Pseudonymisation

Quelles mesures de sécurité organisationnelles ?

- Formations / sensibilisations
- Clause RGPD dans les contrats
- Comité d'éthique
- Engagement de confidentialité

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

Qu'est-ce qu'un transfert de données ? Suis-je concerné(e) ?

1) L'exportateur doit être soumis au RGPD
2) Données accessibles/partagées à un destinataire situé hors de l'UE
3) Destinataire est une entité distincte de l'exportateur et située dans un pays tiers

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

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.

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

Transfert dans l'UE

Autorisation

Transfert hors UE

Interdiction

(sauf 3 exceptions)

Décision d'adéquation

Clauses contractuelles types

Consentement explicite

⚠ Si vous êtes concerné(e) par un transfert hors UE, contactez votre DPO !

Fiche 13 : Sous-traitance

Qu'est-ce que la sous-traitance ? Suis-je concerné(e) ?

- Le fait de mandater un tiers (personne physique ou morale) pour effectuer tout ou partie du traitement de données personnelles, en votre nom et pour votre compte.
- Est-ce que je confie un traitement de données personnelles à un prestataire ? (réalisation d'une enquête, analyse des résultats, réalisation d'un film etc.)

Quelle importance me concernant ?

Vous devez 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.

Comment remplir la fiche du registre de traitement ?

À indiquer : l'identité du prestataire engagé, son rôle et sa finalité d'intervention, les données auxquelles il aura accès, la durée prévue de la prestation et la copie du contrat de sous-traitance.

Pour vous aider, votre DPO peut vous fournir des clauses RGPD types à intégrer dans votre contrat de sous-traitance, ainsi que l'engagement de confidentialité figurant en annexe du guide.

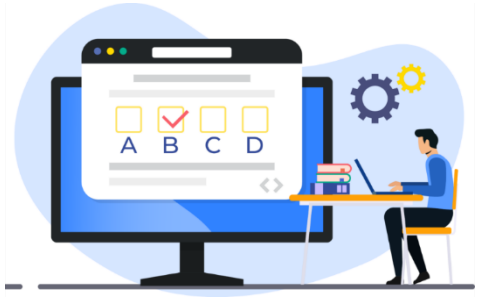
Fiche 11 à 13

Q13 : En matière de sécurité des données, le RGPD impose-t-il une obligation de résultat ou de moyens ?

Il s'agit d'une obligation de moyens de mettre en œuvre des mesures de sécurité proportionnelles aux risques identifiés.

Q14 : Pourquoi le RGPD impose-t-il des restrictions et un encadrement sur le partage des données personnelles en dehors de l'UE ?

Car les règles de protection des données varient d'un pays à l'autre, et certains pays n'offrent pas une protection équivalente à celle du RGPD au sein de l'UE.



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) ?

Analyse de risque, obligatoire dans certaines conditions, qui permet d'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.

Quand dois-je réaliser une AIPD ?

Traitement susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées (2 critères) :

- Traitement de données sensibles
- Traitement concernant des personnes vulnérables
- Traitement de données à grande échelle
- Croisement de données provenant de différentes sources
- Limitation des droits des personnes
- Prise de décision automatisée
- Surveillance systématique des personnes

Comment réaliser une AIPD ?

Identifier les risques pouvant compromettre l’intégrité, la confidentialité ou la disponibilité des données personnelles

↓

Décrire les scénarios pouvant conduire à ces risques et analyser leur gravité et leur probabilité.

↓

Mettre en place des mesures de sécurité adaptées pour atténuer les risques identifiés

Vous êtes concerné par une AIPD ? Contactez votre DPO pour vous faire accompagner !

Ressources

- **Guide de conformité RGPD pour la recherche à Paris 1 en SHS** : demandez-le directement à votre DPO !

- Texte du RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

- Texte de la Loi informatique et libertés : https://www.cnil.fr/fr/la-loi-informatique-et-libertes

- Pages de la CNIL « Recherche scientifique (hors santé) : https://www.cnil.fr/fr/recherche-scientifique-hors-sante

- MOOC de la CNIL : https://www.my-mooc.com/fr/mooc/atelier-rgpd/

L'atelier est composé de 5 modules d'une durée totale de 5 heures environ.

Rebecca ROUSSEAU, adjointe DPO et RSSI
En charge de l'ensemble du volet recherche
DSIUN-CCP : Cellule cybersécurité et protection des données

Contacts :
rebecca.rousseau@univ-paris1.fr
dpo@univ-paris1.fr

PANTHÉON SORBONNE
UNIVERSITÉ PARIS 1