**FICHE D’INSTRUCTION**

**CONFORMITÉ AU RGPD D’UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL**

**DANS LE CADRE D’UN PROJET DE RECHERCHE**

**CONTEXTE ET OBJECTIFS**

Le Règlement Général sur la Protection des Données (RGPD), entré en vigueur le 25 mai 2018, a profondément modifié la législation relative aux données à caractère personnel (DCP).

Dans le cadre de votre projet de recherche, il est possible que vous utilisiez des données personnelles, c’est-à-dire des informations permettant ***l’identification directe ou indirecte d’une personne***. Cette utilisation entraîne diverses démarches et obligations auxquelles vous devez vous conformer tout au long de votre projet, notamment en application du RGPD (Règlement UE 2016/679), de la loi n° 2018-493 du 20 juin 2018, et du décret n° 2018-687 du 1er août 2018.

**Les sanctions élevées prévues en cas de non-conformité rendent indispensable le respect de la réglementation**. Ce questionnaire a pour but d’aider la Mission DPO du périmètre mutualisé à comprendre et encadrer le traitement des DCP dans votre projet. Le Délégué à la Protection des Données (DPD ou DPO) et son équipe pourront ainsi vous accompagner dans les démarches à suivre et les contraintes associées.

Ce questionnaire permet non seulement de recenser et d'analyser le traitement de données à caractère personnel mis en œuvre, mais aussi d'identifier précisément les flux de données et les parties prenantes. Il contribue également à la tenue du registre des activités de traitement, une obligation pour l’Université, et à documenter votre conformité au RGPD.

Il est crucial de réfléchir à la gestion des données personnelles dès l’aune de votre projet de recherche. En effet, la réglementation exige que la protection des données soit intégrée dès la conception du projet. Des délais peuvent être nécessaires en fonction de la complexité de votre dossier, donc n'attendez pas la mise en œuvre du projet pour vous y pencher.

Enfin, avant de soumettre le questionnaire rempli à l'adresse \*\*dpo@grenet.fr\*\*, assurez-vous d'y joindre tous les documents pertinents (note d’information, formulaire de consentement, convention de partenariat, protocole de recherche…).

Date :

Version :

Nom et prénom du répondant :

Laboratoire et adresse électronique :

Directeur du laboratoire et contrat de rattachement du directeur :

Nom du traitement :

**Responsable de traitement**

Le Responsable de traitement est la personne physique ou morale qui détermine les finalités et les moyens du traitement, c’est le Laboratoire représenté par son directeur.

Dans le cadre de recherches menées au sein d’unités mixtes de recherches, il convient d’identifier préalablement à toute démarche à quel établissement le directeur du laboratoire est rattaché afin de déterminer sur quel registre et auprès de quel DPO le traitement de données sera enregistré.

Nom du Directeur

Établissement de rattachement

Nom de l’entité déclarante :

DPO : Déléguée à la protection des données mutualisée des Universités Grenoble Alpes et Savoie Mont Blanc, Grenoble INP et Sciences Po Grenoble

Domaine Universitaire

31 rue des mathématiques

38400 Saint-Martin-d’Hères

06 83 06 16 48/ 04 56 52 90 30

**dpo@grenet.fr**

Relais DPO :

Université Grenoble Alpes : [relaisdpo@univ-grenoble-alpes.fr](mailto:relaisdpo@uni-grenoble-alpes.fr)

Université Savoie Mont Blanc : relaisdpo@univ-smb.fr

Grenoble INP-UGA : relaisdpo@grenoble-inp.fr

Sciences Po Grenoble -UGA : [lynda.maurice@iepg.fr](mailto:lynda.maurice@iep.fr)

**Description du traitement**

Description du traitement (décrire précisément ce que vous faites avec les données des personnes, dites « personnes concernées ») :

Ce traitement est :

☐     déjà mis en place

☐     envisagé

Dans le cadre de cette activité, recueillez-vous directement - en interne - les données auprès des personnes concernées (collecte directe) ? Un organisme externe vous transfère-t-il ces données (collecte indirecte) ? Ou les deux ?

☐     non déterminé

☐     collecte directe

☐     collecte indirecte

    ☐ les deux

Source des données : par quel(s) moyen(s) sont collectées les données des personnes ? :

Estimez le nombre de personnes concernées par ce traitement (si pas de nombre précis, veuillez donner une estimation) :

Date de mise en œuvre du traitement : JJ/MM/AA

Date de mise à jour du traitement : JJ/MM/AA

Quels sont les supports utilisés dans la réalisation de ce traitement ? (outils numériques à spécifier) :

**Pour tout outil numérique, joindre la documentation descriptive : cahier des charges, analyse d’opportunité...**

**Les acteurs**

**1. Le référent opérationnel** qui maîtrise l’activité décrite dans cette fiche de traitement et est en mesure de la décrire dans ce questionnaire :

Nom, prénom :

Adresse mail :

**2. Une ou plusieurs autres organisations sont conjointement responsables** du traitement avec votre établissement. Identifiez chaque acteur co-responsable de traitement et **joindre la convention de coresponsabilité** qui détermine les droits et obligations de chacune des parties :

Nom de l’organisme :

Adresse :

Coordonnées du contact :

Commentaires :

**Finalités**

Quels sont les objectifs poursuivis (les finalités) ? : (exemple de sous finalités liées au projet de recherche : gestion administrative du projet de recherche, publication, animation de conférence, partage de jeux de données)

Finalités Description

1

2

3

N

**LA LICEITE DU TRAITEMENT**

La licéité du traitement signifie que le responsable de traitement traite les données de manière licite, loyale et transparente.

Pour cela, le traitement doit être effectué en se fondant sur l’un des fondements suivants ;

Quel fondement juridique vous donne le droit de traiter les données personnelles ?

Pour pouvoir être mis en œuvre, le traitement doit se fonder sur au moins une des six bases légales prévues par l’article 6 du RGPD. Merci de bien vouloir cocher le fondement juridique sur lequel se base le traitement :

☐ le consentement des personnes *Préciser les modalités de collecte, de conservation et de retrait*

*du consentement*

☐ le contrat (joindre le contrat en question) Données *nécessaires pour assurer la bonne exécution du contrat*

☐ l’obligation légale (joindre les textes légaux qui l’imposent)

☐ la sauvegarde des intérêts vitaux

☐ la mission d’intérêt public

☐ l’intérêt légitime de l’établissement

Si le traitement est fondé sur le consentement de la personne, êtes-vous en mesure de transmettre, dès maintenant, les formulaires que vous envisagez d’utiliser dans le cadre du projet de recherche ?

☐ Oui

☐ Non (indiquez les délais dans lesquels vous seriez en mesure de les fournir) ……………………………………

……………………………………. …………………………………………………………...

**Personnes**

Quelles sont les personnes dont vous recueillez les données ? (Étudiants, personnels, candidats, mineurs, sujets d’étude…) :

Les personnes concernées sont « les personnes physiques identifiables ou identifiées dont les données à caractère personnel sont collectées et intégrées dans le traitement de données à caractère personnel ».

Les personnes concernées peuvent appartenir à plusieurs catégories : par ex. pour une recherche en santé : patients, aidants, médecins, infirmiers...

- Enseignants/chercheurs

- Doctorants/post-doctorants

- Salariés/agents

- Fournisseurs

- Intérimaires

- Partenaires

- Stagiaires

- Prestataires

- Étudiants/auditeurs

- Prospects

- Visiteurs

- Adhérents

- Clients

- Autres (précisez)

Mineurs :

Le traitement concerne-t-il des données de personnes de moins de 16 ans ?

- Exclusivement

- En partie

- Jamais

Description des modalités de recrutement (s’il y a lieu) :

**Destinataire(s) des données**

Qui accède à tout ou partie des données personnelles ou peut recevoir des extractions de ces données ?

☐ service interne qui traite les données

☐ d’autres services internes

☐ sous-traitants (les entités externes qui gèrent les données personnelles pour le compte de votre établissement).

Indiquez si un contrat existe précisant les modalités de traitement des données personnelles par les parties :

☐ cadre juridique existant **(joindre le contrat)**

☐ destinataires dans des pays tiers ou organisations internationales

☐ partenaires institutionnels ou commerciaux

☐ autre (préciser)

Commenter, préciser ou qualifier l’activité assurée par le destinataire :

**LA SOUS TRAITANCE**

La notion de de sous-traitance s’entend par le fait que « la personne physique ou morale, l'autorité publique, le service ou un autre organisme traite des données à caractère personnel pour le compte du responsable du traitement ».

Attention, il ne s’agit pas de sous-traitance au sens technique du terme mais au sens du RGPD ;

Nom et coordonnées du sous-traitant

Type(s) d’intervention(s)

Existe-t-il un contrat ? Oui ☐ Non ☐ Si non, justifier :

- Si non, justifier :

Le sous-traitant a-t-il désigné un DPO ?

Oui ☐ Non ☐

Le sous-traitant dispose-t-il d’un registre des traitements sous-traitant ? Oui ☐ Non ☐

Existe-t-il des flux de données hors de l’Union européenne ?

Les flux en dehors de l’UE doivent être clairement identifiés Oui ☐ Non ☐

- Si oui, préciser :

- Existe-t-il des sous-traitants ultérieurs ?

**Données**

A quelle catégorie de données personnelles appartiennent les données collectées ?

**Pour chaque catégorie, précisez les données exactes**

☐ état civil, identité, données d’identification (nom, prénom, adresse, photographie, date et lieu de naissance...):

☐ vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses) :

☐ vie professionnelle (CV, scolarité, formation professionnelle, distinctions…) :

☐ informations d’ordre économique et financier (revenus, situation financière, fiscale…) :

☐ données de connexion (adresse IP, journaux d’évènements…) :

☐ données de localisation (déplacements, données GPS…) :

☐ coordonnées bancaires :

☐ autres (cookies, vidéos…):

**Données dites sensibles (ne pouvant pas être collectées sauf exceptions) :**

La notion de **données sensibles** s’entend de « toutes données à caractère personnel qui révèlent l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que toutes données génétiques, toutes données biométriques aux fins d'identifier une personne physique de manière unique, et toutes données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

Il faut intégrer dans les données sensibles le numéro de sécurité sociale ainsi que les données relatives aux condamnations pénales et aux infractions (exemple : infraction au code de la route pour les voitures de fonction).

Les sanctions internes ne sont pas considérées comme faisant partie des infractions au sens du RGPD.

☐ données révélant l’origine raciale ou ethnique :

☐ données révélant les opinions politiques :

☐ données révélant les convictions religieuses ou philosophiques

☐ données révélant l’appartenance syndicale

☐ données génétiques :

☐ données biométriques aux fins d’identifier une personne physique de manière unique :

☐ données concernant la santé :

☐ données concernant la vie sexuelle ou l’orientation sexuelle :

☐ données relatives à des condamnations pénales ou infractions :

☐ numéro d’identification national unique (NIR) (numéro de sécurité sociale)

**A compléter en cas de traitement de données sensibles :**

| Données sensibles | Origine / source | Durée de  conservation | Destinataires |
| --- | --- | --- | --- |
| Préciser le détail des données pour chaque catégorie | D’où proviennent les données ?  collecte directe auprès de la personne (ex. réponses à un questionnaire), collecte indirecte (à partir d’un traitement existant, transmises par un tiers, …) | Durée pendant la laquelle les données sont conservées et justification de la durée. | Destinataires internes ou externes de ces données,  Indiquer les organismes, services ou personnes destinataires |
|  |  |  |  |

Utilisez-vous une ou des zones de commentaires libres ? ☐ Oui ☐ Non

*Une zone de commentaire (ou champ libre) permet de soumettre des observations sur la personne concernée et permet les commentaires subjectifs comme « candidat ennuyeux, sérieux, pas sérieux… »*

Combien de temps sont conservées les données personnelles et où ? :

**Listez les différentes durées en fonction des données personnelles et des finalités, il faut compléter autant de tableaux que de finalités identifiées**

| Finalité 1 | | | |
| --- | --- | --- | --- |
| Catégorie de données | Détail des données | Durée de  conservation | Destinataires |
| État civil, identité, données d'identification… |  |  |  |
| Images (trombinoscopes, vidéosurveillance…) |  |  |  |
| Vie personnelle  (habitudes de vie,  situation familiale,  etc.) |  |  |  |
| **Vie professionnelle (CV, scolarité, formation professionnelle, distinctions, adresse mail professionnelle, etc.)** |  |  |  |
| Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) |  |  |  |
| Données de connexion (adresses IP, logs, etc.) |  |  |  |
| Données de localisation (déplacements, données GPS, GSM, etc.) |  |  |  |
| Numéro de Sécurité  sociale ou NIR |  |  |  |
| Autres données |  |  |  |

**Mesures juridiques**

Quelles mesures de nature juridique avez-vous mises en place ?

**Décrivez précisément chaque mesure mise en œuvre :**

☐ Finalité : finalité déterminée, explicite et légitime :

☐ minimisation : réduction des données à celles strictement nécessaires :

☐ qualité : préservation de la qualité des données personnelles :

☐ durées de conservation : durée nécessaire à l’accomplissement des finalités, à défaut d’une autre obligation légale imposant une conservation plus longue :

☐ information : respect du droit à l’information des personnes concernées :

**Précisez les moyens d’information aux personnes et joindre les documents d’information**

**☐** transferts : respect des obligations en matière de transfert de données en dehors de l’Union européenne :

**Joindre la documentation associée au transfert**

**Mesures organisationnelles**

Quelles mesures organisationnelles avez-vous mises en place ?

**Décrivez précisément chaque mesure mise en œuvre :**

☐ organisation pour assurer la protection des données : **décrivez les flux de données :**

☐ gestion des risques :

Après revue par la direction Métier, le RSSi et le DPO, le traitement a été évalué conforme à la politique de sécurité des systèmes d'information de l’établissement

Accès aux données limité aux personnels habilités : **décrivez le processus d'habilitation :**

☐ Encadrement des relations avec les tiers :

☐ autre :

Commentaires :

**Mesures de sécurité logique**

Quelles mesures de sécurité logique avez-vous mises en place ?

**Décrivez précisément chaque mesure mise en œuvre :**

☐ anonymisation :

☐ chiffrement :

☐ contrôle d’intégrité :

☐ sauvegardes :

☐ cloisonnement (données, réseau) :

☐ contrôle d’accès logique :

☐ traçabilité :

☐ exploitation :

☐ surveillance (paramétrages, contrôles de configuration, surveillance en temps réel…) :

☐ gestion des postes de travail :

☐ lutte contre les codes malveillants (virus, logiciels espions…) :

☐ protection des canaux informatiques (réseaux) :

☐ pseudonymisation :

Commentaires :

**Mesures de sécurité physique**

Quelles mesures de sécurité physique avez-vous mises en place ?

**Décrivez précisément chaque mesure :**

☐ contrôle d’accès physique :

☐ sécurité des matériels :

☐ sécurité des documents papier :

☐ sécurité des canaux papier :

☐ protection contre les sources de risques non humaines (feu, eau…) :

Commentaires :

**Transfert des données hors UE**

Des données personnelles sont-elles transmises hors de l’Union européenne ?

NON ☐ OUI ☐

Si oui, précisez le(s) destinataire(s) situé(s) en dehors de l’Union Européenne :

Vers quel(s) pays ?

Quel type de garantie a été mis en place pour sécuriser le transfert ?

☐ certification

☐ clauses contractuelles types (CCT)

☐ codes de conduite

☐ décision d’adéquation

☐ dérogation pour des situations particulières

☐ autres :

Justifiez le choix d'un hébergement éloigné et indiquez les modalités d'encadrement juridique mises en œuvre afin d'assurer une protection adéquate aux données :

**Facteurs de risque**

Votre traitement répond -il à un ou plusieurs de ces critères ?

☐ vous établissez des profils, des évaluations, des notations de personnes

☐ l'outil utilisé pour votre activité permet de prendre une décision automatisée avec effets légaux sur la personne concernée à l'aide d'algorithmes appliqués à ses données personnelles et sans intervention humaine

☐ l'outil utilisé pour votre activité permet d'assurer la surveillance systématique de personnes

☐ vous collectez un large volume de données personnelles pour cette activité de traitement, qui s'étend sur un large périmètre géographique, se poursuit dans le temps

☐ vous faites des recoupements entre les données de différentes bases de données collectées pour atteindre différents objectifs

☐ votre activité sur les données concerne des personnes vulnérables : mineurs, employés...

☐ vous utilisez une technologie innovante

☐ l’outil utilisé pour votre activité permet d'autoriser, de modifier ou de refuser l'accès à un service ou la conclusion d'un contrat (avec des fonctionnalités de filtrage)

☐ vous collectez des données de santé

Le traitement est-il exonéré de l'obligation de mener une analyse d'impact relative à la protection des données ?

NON ☐ OUI ☐

**Les bonnes pratiques en matière de sécurité**

Avez-vous pensé à :

|  |  |
| --- | --- |
| Sensibiliser les utilisateurs | * Les personnes manipulant les données sont informées et sensibilisées (engagement de confidentialité par exemple) |
| Authentifier les utilisateurs | * Définir un identifiant unique à chaque utilisateur adopter une politique de mots de passe * Obliger l’utilisateur à changer son mot de passe régulièrement * Limiter le nombre de tentatives d’accès à un compte |
| Gérer les habilitations | * Définir les profils d’habilitation * Supprimer les permissions d’accès obsolètes * Réaliser une revue bi-annuelle des habilitations |
| Tracer les accès et  gérer les incidents | * Prévoir un système de journalisation, et en informer les utilisateurs * Protéger les informations de journalisation * Prévoir une procédure de notification de violation de données personnelles |
| Sécuriser les postes de travail | * Prévoir le verrouillage automatique de session * Utiliser des antivirus à jour * Installer un pare feu logiciel |
| Sécuriser les serveurs | * Limiter l’accès aux outils d’administration aux seules personnes habilitées * Installer sans délai les mises à jour critiques |
| Sécuriser les sites web | * Utiliser le protocole TLS * Vérifier qu’aucun mot de passe ou identifiant ne passe dans les url * Mettre un bandeau de consentement pour les cookies non nécessaires au service, le cas échéant |
| Sauvegarder et prévoir la continuité d’activité | * Effectuer des sauvegardes régulières * Stocker les supports de sauvegarde dans un endroit sécurisé |
| Archiver de manière sécurisée | * Mettre en œuvre des accès spécifiques aux données archivées * Détruire les archives obsolètes de manière définitive |
| Encadrer la maintenance et la destruction des données | * Enregistrer les interventions de maintenance dans une main-courante * Effacer les données de tout matériel avant sa mise au rebut * Encadrer les interventions par des tiers |
| Sécuriser les échanges avec l’extérieur | * Chiffrer les données avant envoi * S’assurer qu’il s’agit du bon destinataire * Transmettre le secret lors d’un envoi distinct et via un canal différent |
| Protéger les locaux | * Restreindre l’accès par des portes verrouillées et/ou du contrôle d’accès |
| Encadrer les développements informatiques | * Éviter les zones de commentaires ou les encadrer * Tester sur des données fictives ou strictement anonymes |
| Utiliser des fonctions cryptographiques | * Utiliser des logiciels reconnus * Chiffrer les données ou le disque dur de votre pc portable * Conserver les secrets et les clés cryptographiques de manière sécurisée |