#

# Renseignements relatifs à la confOrmité AU rgpd

# d’un traitement de données à caractere 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, modifie le droit des données à caractère personnel (« DCP »).*

*Votre projet de recherche peut induire l’utilisation de données personnelles, c’est à dire de* ***données permettant l’identification directe ou indirecte de personnes****. L’utilisation de ces données induit un certain nombre de démarches et d’obligations auxquelles vous êtes tenus tout au long de votre projet, notamment en application du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (modifiant la**loi n° 78-17 du 6 janvier 1978) et du Décret no 2018-687 du 1er août 2018.*

*Le montant très élevé des sanctions que risquent les acteurs en cas de manquement aux nouvelles obligations rend indispensable la conformité avec la règlementation applicable.*

*Le présent questionnaire est un outil mis à votre disposition afin de permettre à l’équipe en charge de la protection des données personnelles de l’Université de connaître le traitement des DCP que vous mettez en œuvre. Ainsi le délégué à la protection des données (« DPD » ou Data Protection Officer « DPO »)* *ou son équipe vous éclaireront sur la formalité déclarative du traitement, et les contraintes qui y sont liées. C’est un document de recensement et d’analyse, elle doit refléter la réalité de vos traitements et permettre d’identifier précisément le flux des données et les intervenants.*

*La tenue d’un registre des activités de traitement par l’Université, obligatoire, et la situation créée par la nature et le flux des données impliquées dans la recherche obligent à recueillir les informations recensées par ce questionnaire. Le questionnaire est aussi un outil de démonstration de votre conformité au RGPD. Il permet de documenter vos traitements de données et de poser les questions : ai-je besoin de cette donnée? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ?*

*Il est impératif de travailler sur la question des données personnelles* ***dès le début du projet de recherche, sans attendre la mise en œuvre de celui-ci****. La réglementation en vigueur impose en effet que les données soient protégées dès leur conception. Il est donc essentiel de* ***ne pas attendre le moment du lancement du projet****, sachant que* ***des délais, qui peuvent être importants en fonction de la complexité d’un dossier****, seront nécessaires.* *Les contraintes augmentent avec les risques encourus par les personnes concernées.*

*Enfin, avant de retourner la fiche remplie à* *dpo@u-bordeaux.fr**, ne manquez pas d’adjoindre les documents utiles au diagnostic du traitement : note d’information des personnes, formulaire de consentement, convention de partenariat, protocole de recherche…*

|  |  |
| --- | --- |
| Date |   |
| Version |   |
| Nom et prénom de la personne répondant au questionnaire |  |
| Laboratoire de rattachement et adresse mail |   |

2. IDENTIFICATION DU TRAITEMENT

|  |  |
| --- | --- |
| Nom du traitement en interne *(acronymes à détailler)* |   |
| Dénomination commerciale de l’éditeur et nom del’application  |   |
| Version |   |
| Date de mise en service  |   |
| Editeur *(en cas de développement interne, indiquer le service concerné)* |   |
| Maintenance  |   |

1. DESCRIPTIF SYNTHÉTIQUE DU TRAITEMENT

*Veuillez indiquer l’objet de la recherche impliquant les DCP ainsi que leur usage au sein de cette recherche :*

1. RESPONSABLE DU TRAITEMENT

*Le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».*

*Le responsable du traitement est donc celui qui identifie les objectifs principaux du traitement et les moyens utilisés pour mettre en œuvre ce traitement.*

|  |  |
| --- | --- |
| Nom et coordonnées du responsable du traitement  |   |
| Eventuellement : co-responsable de traitement **/!\** *Il y a co-responsabilité**dans le cas où un ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement. Ne pas confondre avec la sous-traitance (voir point n° 10)* | Non ☐Oui ☐ Si oui, préciser le nom et les coordonnées : |
| Nom et coordonnées du service ou de la personne en charge du traitement s’il estdifférent du responsable du traitement  |   |

1. FINALITÉS DU TRAITEMENT

*La finalité d’un traitement est définie comme étant les « objectifs principaux assignés au traitement et aux fonctions substantielles mises en œuvre » par le responsable de traitement ou le sous-traitant.*

|  |  |
| --- | --- |
| Finalités | Description |
|  1  |   |
|  2  |    |
| 3 |    |
| N |     |

1. PERSONNES CONCERNÉES

*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   |  ☐ |
| Intérimaire | ☐ | Partenaires   | ☐ |
| Stagiaire   | ☐ | Prestataires   | ☐ |
| Étudiants /auditeur  | ☐ |  Prospects  | ☐ |
| Visiteurs  | ☐ |  Adhérents  | ☐ |
| Clients | ☐ |  Autres *(préciser)* | ☐ |

**Mineurs**:

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

* exclusivement ☐
* en partie ☐
* jamais ☐

Nombre approximatif de personnes concernées : …………………….

Mode de recrutement des personnes concernées (s’il y a lieu) :

**Votre projet de recherche implique-t-il une mobilité ?**

 Non

 Oui (*décrivez sommairement : personnes concernées et mode de gestion de la mobilité*) …………………………………………………………………………………………

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

1. COLLECTE DE DONNÉES SENSIBLES

*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.*

**Collectez-vous des données sensibles ?**

| Données sensibles | Origine / source | Durée de conservation | Destinataires |
| --- | --- | --- | --- |
| Préciser le détail des données pour chaque catégorie de donnée retenue dans le tableau précédent | 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 nécessairesau traitement et au delà de laquelle elles sont supprimées (préciser si routine d’effacement) | destinataires internes ou externes de ces données,Indiquer les organismes, services ou personnes destinataires |
| Origine raciale |  |  |  |
| Opinions politiques |  |  |  |
| Convictions religieuses |  |  |  |
| Convictions philosophiques |  |  |  |
| Appartenance syndicale |  |  |  |
| Données génétiques |  |  |  |
| Données biométriques aux fins d’identification d’une personne |  |  |  |
| Données concernant la santé |  |  |  |
| Données concernant la vie sexuelle  |       |  |       |
| Numéro de sécurité sociale |  |  |  |
| Infractions ou condamnations pénales |  |  |  |

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… »*

1. DONNÉES COLLECTÉEs, origine, conservation, destinataires

*La notion de donnée personnelle s’entend de « toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». La notion de catégorie de données à caractère personnel s’entend d’un ensemble de données pouvant être regroupées au sein d’une même famille*.

 Préciser les données collectées (le détail) et la catégorie de personnes concernées par cette collecte.

| 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 |  |  |  |

*La notion de durée de conservation s’entend par le fait que « les données sont conservées par le responsable de traitement sous une forme permettant l’identification des personnes concernées pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».*

*Les durées de conservation des données peuvent être différentes par catégories*.

*Les destinataires des données s’entendent de toute « personne physique ou morale, l'autorité publique, service ou tout autre organisme qui reçoit communication de (toutes ou partie des) données à caractère personnel, qu'il s'agisse ou non d'un tiers. »*

*Ex. de destinataires : une filiale, un établissement partenaire, un sous-traitant, etc*.

|  |  |  |  |
| --- | --- | --- | --- |
| Données ou catégories | Origine / source | Durée de conservation | Destinataires |
| Préciser le détail des données pour chaque catégorie de donnée retenue dans le tableau précédentex. : coordonnées :Adresse postale, tél. | D’où proviennent les données ?\*Indiquer les organismes **et** les traitements sources des flux de données entrants (via des applications par ex.)Ex. collecte directe auprès de la personne (ex. réponses à un questionnaire), collecte indirecte (à partir d’un traitement existant, transmise par un tiers, …)  | Durée pendant la laquelle les données sont nécessairesau traitement et au-delà de laquelle elles sont supprimées (préciser si routine d’effacement) | Quels **destinataires internes ou externes**  pour quelles **catégories** de données ?Indiquer les organismes **et** les traitements destinataires des flux de données sortants (via des applications par ex.). Préciser, s’il y a lieu, les transferts de données hors de l’Union européenne. |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |
|       |       |  |       |
|       |       |       |       |
|       |       |       |       |

9. lICEITE DE LA COLLECTE DES DONNÉES

*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 :*

Consentement de la personne ☐

*Préciser les modalités de collecte, de conservation et de retrait*

*du consentement*

Exécution d’un contrat ☐

*Données nécessaires pour assurer la bonne exécution du contrat*

Respect d’une obligation légale ☐

*Données fiscales pour l’administration fiscale,*

*données traitées par un établissement hospitalier, etc.*

Sauvegarde des intérêts vitaux de la personne ☐

Réponse à une mission d’intérêt public ☐

Données scolaires, prestations sociales, etc.

Intérêt légitime du responsable de traitement ☐

Intérêt légitime du responsable de traitement (ex : gestion du personnel pour les données RH)

**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*) ……………………………………

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

10. 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.*

 ☐ Non, le traitement ne fait pas l’objet d’une sous-traitance

☐ Oui, le traitement fait l’objet d’une sous-traitance dans les conditions suivantes :

|  |  |
| --- | --- |
| 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[[1]](#footnote-1) ?*Les flux en dehors de l’UE doivent être clairement identifiés*  | Oui ☐ Non ☐- Si oui, préciser : |

11. SECURITE

*Le RGPD impose que « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».*

Avez-vous pensé à :

|  |  |  |
| --- | --- | --- |
| Sensibiliser les utilisateurs | * Les personnes manipulant les données sont informées et sensibilisées
 | ☐ |
| 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 etgérer 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
 | ☐☐☐ |
| 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
 | ☐☐☐ |
| Gérer la sous-traitance | * Voir § 10
 | ☐ |

Décrivez l’architecture informatique du traitement : type d’ordinateurs : perso ou pro, fixe ou portable, client, serveur, type de réseaux (filaire, wifi privé ou non,..), type de supports utilisés pour les données (disque durs, USB, ..), les formats des données (xls, csv, txt, …), les moyens de transferts ou échanges de données, (clé, pièce jointe chiffrée), les types et la fréquence de sauvegardes…) et toutes autres informations que vous jugerez utiles.

12. ANALYSE D’IMPACT et RIPH

*L’article 35 du RGPD considère que* « *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* ».

Évaluation / scoring (évaluation d’aspects personnels ou notation

d’une personne,  y compris le profilage) ☐

Décision automatisée avec effet légal ou similaire (exemple : décision prise

à l’égard d’une personne par le biais d’algorithmes appliqués aux données,

sans intervention humaine)  ☐

Surveillance systématique (exemple : télésurveillance) ☐

Collecte de données sensibles (exemple : santé, biométrie, etc.) ☐

Collecte de données personnelles à large échelle (volume important de données

collectées au niveau régional, national, ou international) ☐

Croisement de données (pluralités des sources des données) ☐

Personnes vulnérables (patients, personnes âgées, mineurs, etc.) ☐

Usage innovant ou application de nouvelles technologies

(par ex. : objets connectés, télétravail…) ☐

Exclusion du bénéfice d’un droit, d’un service ou d’un contrat ☐

*Une Recherche Impliquant la Personne Humaine (RIPH)* *est une recherche organisée et pratiquée sur des personnes saines ou malades en vue du développement des connaissances biologiques ou médicales.*

Les données sont-elles collectées dans le cadre d’une RIPH ?

 Oui

 Non

Si vous avez répondu oui à la question précédente, indiquer s’il s’agit de :

 Recherche interventionnelle

 Recherche interventionnelle à risque et contrainte minimes

 Recherche non interventionnelle

 Ne sait pas

Indiquer le nom du promoteur de cette RIPH :

…………………………………………………………………………………………...

13. Droits des personnes

13,1 DROIT A L’INFORMATION

*Les personnes concernées doivent être informées de la finalité du traitement*.

Les personnes ont-elles été informées de la collecte de leurs données pour cette finalité ? ☐

Comment ?

Mentions d’information sur support de collecte ☐

note (ou lettre) d’information ☐

note de service ☐

Affichage ☐

 Autre ☐

## 13,2 droits d’acces, d’opposition et rectification

*Le responsable de traitement est tenu d’indiquer aux personnes concernées les modalités d’exercice de leurs droits d’accès, d’opposition, de rectification de leurs données.*

*Les personnes concernées ont le droit d’avoir accès à leurs données, d’obtenir la rectification, l’effacement des données les concernant, elles ont le droit ne pas faire l’objet d’un profilage*.

Les personnes ont-t-elles été informées des modalités d’exercice de leurs droits d’accès et d’opposition, rectification ? ☐

Ont-elles été informées de la fonction de la personne et des coordonnées du service

auprès desquels exercer ce droit ? ☐

Ont-elles la possibilité de définir le sort de leurs données après leur mort ? ☐

## 13,3 portabilitE

*Le RGPD instaure le droit à la portabilité des personnes concernées par le traitement de leurs DCP. Si votre traitement cumule les trois règles suivantes, vous devrez permettre à la personne concernée l’exercice de ce droit et lui fournir sous un format adéquat ses données personnelles »*

Données fournies par la personne concernée elle-même ☐

Le traitement est fondé soit sur la base du consentement

(article 6.1.a) ou article 9.2.a)), soit sur un contrat (article

6.1.b)). ☐

Le traitement est automatisé ☐

14. cadre juridique DE LA RECHERCHE

Votre projet de recherche implique-t-il plusieurs Laboratoires / Universités / Partenaires publics ou privés ?

 Oui (*dans l’affirmative, merci de préciser quelles structures sont impliquées et quelle est leur forme juridique : établissement public d’enseignement supérieur, sociétés, associations, établissements publics, etc.*)

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

 Non

Listez les conventions qui vous lient dans le cadre de ce projet de recherche (accords de partenariats, de consortium, protocoles, etc.) :

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

Parmi ces instruments, quels sont ceux qui sont assortis de dispositions concernant le traitement des DCP (clauses dans la convention, annexe ou avenant) ?

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

Etes-vous en mesure de transmettre, dès maintenant, l’ensemble de ces instruments aux fins d’expertise du projet ?

 Oui

 Non (*indiquez les raisons pour lesquelles vous ne disposez pas de ces instruments et les délais dans lesquels vous seriez en mesure de les fournir*) ……………………………………

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Une fois cette fiche remplie, merci de la retourner à* *dpo@u-bordeaux.fr**,*

*Y joindre éventuellement toute pièce que vous jugerez utile (y compris : schémas, organigrammes…).*

1. Les flux en dehors de l’UE doivent être clairement identifiés [↑](#footnote-ref-1)