Une introduction au RGPD

Gaëlle Coz

MSHS Poitiers

20 juin 2023

Plan de la présentation

- Qu’est-ce-que le RGPD?
- Mise en perspective historique du RGPD
- Les définitions du RGPD
- Les grands principes du RGPD
- Quelle démarche à l’UP pour une mise en conformité ?

Qu’est-ce-que le RGPD ?

Le **R**ègleement **G**énéral sur la **P**rotection des **D**onnées

(en anglais, GDPR – General Data Protection Regulation)

Définition :	Il encadre le **traitement des données à caractère personnel** sur le territoire de l’Union Européenne
Enjeu :	Limiter les risques d’atteinte à la vie privée et aux libertés individuelles
Objectifs :	- Renforcer les droits des personnes - Responsabiliser tous les acteurs - Renforcer les pouvoirs de sanction - Fixer un cadre juridique unifié pour l’ensemble de l’UE

Le contexte historique

1973 Projet du gouvernement d'interconnexion des fichiers de l'administration

1974 Projet **Safari** révélé au public ; Évaluation des risques de l'informatique sur la vie privée

1978 **Loi Informatique et Libertés**
Création de la **Cnil**, Commission Nationale de l'Informatique et des Libertés

1995 **Directive européenne** sur la protection des données personnelles

2004 Réforme de la loi Informatique et Libertés

2016 En France, **Loi pour une République Numériqu**e
En Europe, Adoption du **Règlement Général sur la Protection des Données**

2018 Entrée en vigueur du RGPD

Le périmètre du RGPD

Le RGPD s'applique à **toute organisation, publique ou privée**, qui traite des données à caractère personnel pour son compte ou non, dès lors :

- que l'organisation est établie sur le territoire de l'Union Européenne,
- ou que l'activité de l'organisation vise directement des résidents européens

→ **établissements de recherche** concernés

L'exception domestique

- le RGPD ne s'applique pas aux traitements de données effectués au cours d'activités strictement personnelles (ex : constitution d'un carnet d'adresses privées, publication personnelle sur les réseaux sociaux)
- En revanche l'organisation qui fournit le dispositif dans ce cadre privé est soumis au RGPD

Qu’est-ce qu’une donnée à caractère personnel ?

Une donnée à caractère personnel est **toute information se rapportant à une personne physique identifiée ou identifiable**.

- Toute information, qu’elle soit objective ou subjective, touchant à la vie privée stricto sensu ou plus largement
- Se rapportant à une personne physique, les personnes morales (ex : une entreprise) ne sont pas concernées
- Qui permet d’identifier la personne
  - directement ou indirectement
  - à partir d’une seule donnée ou du croisement de plusieurs données

Des exemples de données personnelles

Identification directe (une seule donnée)	Identification indirecte (une donnée + une table de correspondance)	Identification indirecte par croisement de plusieurs données
Nom Prénom Photo Voix Vidéo Email …	Numéro de téléphone Adresse IP Numéro de sécurité sociale Numéro identifiant dans une table de correspondance …	Âge, adresse, profession Commentaires libres …

Les données personnelles faisant l'objet d'un encadrement spécifique

- Les données dites **sensibles**
- Les données d'infractions ou liées aux condamnations
- Les données concernant les **populations** dites **vulnérables** (mineurs, personnes âgées, patients, réfugiés, prisonniers, salariés enquêtés sur leur établissement professionnel…)
- Le numéro de sécurité sociale

→ Ces données présentent un risque élevé d'atteinte à la vie privée et aux libertés individuelles

→ Des formalités supplémentaires sont à effectuer comme :
Demande de consentement, analyse d'impact, méthodologie de référence, avis de la Cnil

Les données personnelles dites sensibles

- Origine raciale ou ethnique
- Opinions politiques, convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques ou biométriques (traitées uniquement pour identifier une personne)
- Santé
- Vie sexuelle ou orientation sexuelle

Le traitement de ces données est interdit sauf si :

consentement explicite de la personne, données rendues manifestement publiques par la personne concernée, intérêt public important, sauvegarde de la vie humaine, traitement nécessaire à des fins de recherche publique (à justifier)

Les données de santé

Ce 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.
Définition Cnil

Difficulté : Caractériser le type de recherche envisagée pour ensuite identifier la procédure à appliquer

Des données de santé vont être utilisées et la recherche :

- N'est pas dans le domaine de la santé (n'a pas pour effet l'amélioration de la santé)

  → Procédure identique à celle des données sensibles
- A pour objectif l'amélioration de la santé
  - Recherche N'Impliquant pas la Personne Humaine (RNIPH)
  - Recherche Impliquant la Personne Humaine (RIPH)

  → Procédures spécifiques dont les **méthodologies de référence** (MR004 etc)

Aide à la qualification du type de recherche : Guide pédagogique du Health Data Hub

Qu’est-ce qu’un traitement ?

Une opération ou un ensemble d'opérations portant sur des données personnelles

Exemples :

Collecter	Consulter
Enregistrer	Extraire
Structurer	Stocker
Modifier	Transmettre
Manipuler	Diffuser

→ Concerne tout le cycle de vie de la donnée

→ Concerne tous les supports (numérique, papier)

Les acteurs du traitement

Dénominations	Rôles
Le responsable du traitement L'Université de Poitiers, représentée par la Présidente	- Détermine les finalités et les moyens nécessaires à la mise en œuvre du traitement - Endosse la responsabilité pénale
Le référent opérationnel Le chercheur	- Conduit le projet - Effectue les démarches de conformité au RGPD
Le sous-traitant Ex : société de sondage	- Traite des données personnelles pour le compte et sous l'autorité du responsable du traitement - Assure la sécurité et la confidentialité des données
Le délégué à la protection des données Le DPO de l'Université de Poitiers	- Fait respecter le RGPD dans son organisation - Sensibilise et accompagne - Tient le registre des traitements de l'Université
La Cnil, la Commission Nationale Informatique et Libertés	- Accompagne les professionnels et protège les particuliers - Informe - Contrôle l'application du RGPD et sanctionne

Les 8 règles d'or du RGPD

- **Finalité du traitement**
  Les données personnelles collectées ne peuvent être traitées que pour une finalité définie précisément et légitime
- **Licéité du traitement**
  Le traitement doit être fondé sur une base légale
- **Minimisation des données**
  Les données doivent être pertinentes et limitées à ce qui est nécessaire au regard des finalités
- **Protection particulière des données sensibles**
  Les données sensibles ne peuvent être collectées et traitées que sous certaines conditions
- **Obligation de sécurité**
  Au regard des risques, des mesures doivent être mises en œuvre pour assurer la sécurité des données traitées
- **Conservation limitée des données**
  Les données ne peuvent être conservées que pour une durée prédéfinie et limitée
- **Transparence**
  Les personnes doivent être informées de l'utilisation des données les concernant et de la manière d'exercer leurs droits
- **Droits des personnes**
  Les personnes bénéficient de nombreux droits qui leur permettent de garder la maîtrise de leurs données

La finalité

- **Objectif** du traitement
- Doit être **déterminée**

  Permet de définir le périmètre des usages des données

  Pour les recherches en sciences sociales, la problématique de recherche est souvent la finalité du traitement

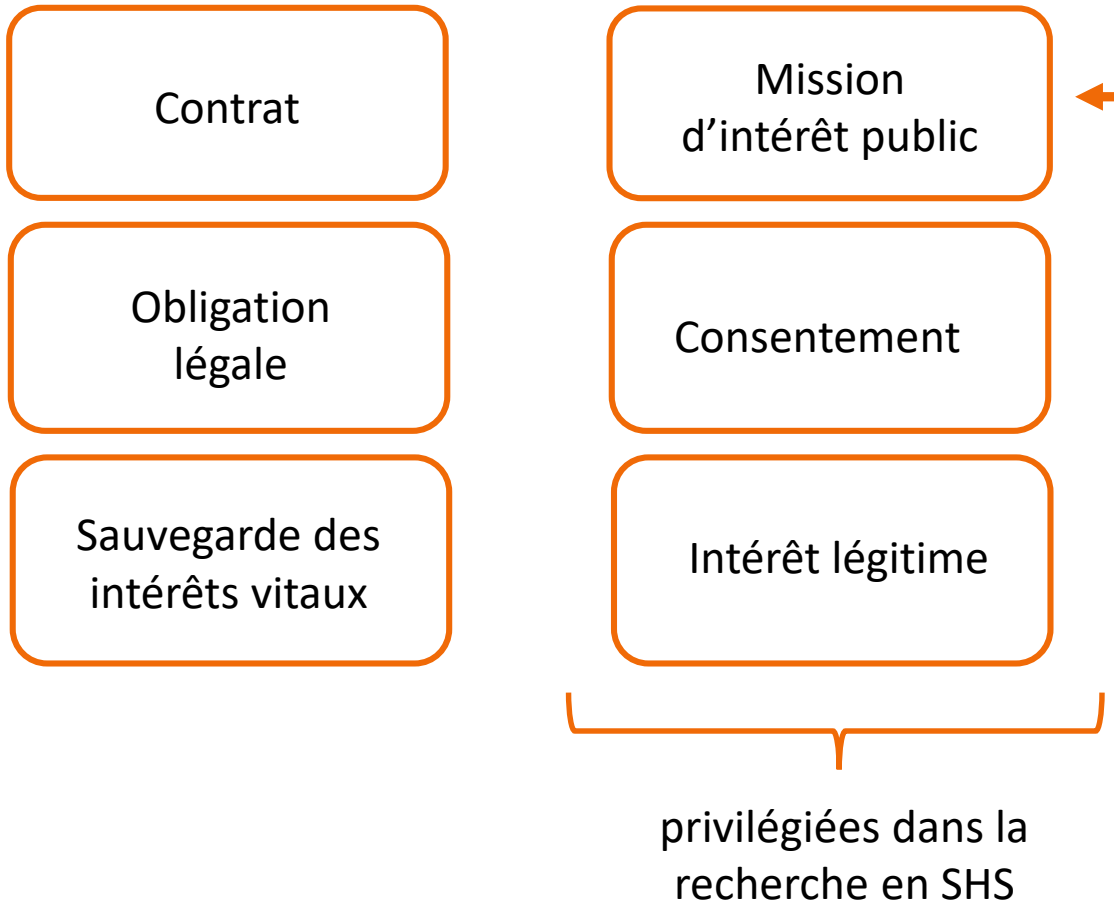
  Une certaine indétermination permise dans le cadre de la recherche

  Peut être large au début du projet puis s'affiner au cours du projet (le préciser au DPO)
- Doit être **légitime**

  Entrer dans le cadre des activités de recherche du laboratoire
- **Principe clé**

  Permet de déterminer la pertinence des données recueillies, de fixer la durée de conservation des données, de déterminer les personnes habilitées à y accéder
- Sanction pénale en cas de détournement de finalité

La licéité ou les bases légales du traitement



Recherche financée sur fonds publics

En pratique, c'est le DPO qui détermine la base légale en lien avec le demandeur et en fonction de la finalité du traitement

Le consentement

- Le RGPD impose que ce consentement soit :
  - **Libre** : non contraint, non influencé
  - **Spécifique** : pour un seul traitement avec ses finalités associées
  - **Éclairé** : accompagné d'informations (finalités, droits de la personne…)
  - **Révocable** : pouvant être retiré à tout moment
  - **Univoque :** sans ambiguïté (pas de cases pré-cochées)
- Lorsque la personne a moins de 15 ans, l'information doit être adaptée et le consentement autorisé par le titulaire de l'autorité parentale
- Il est exigé pour le traitement des données sensibles
- Le responsable du traitement doit conserver la preuve du consentement

La minimisation et l'exactitude des données

- **Minimisation** (ou proportionnalité)

  Ne collecter et ne traiter les données que strictement nécessaires pour atteindre la finalité

  Ex : tranche d'âge plutôt que date de naissance, quartier plutôt qu'adresse complète

- **Pertinence**

  En lien direct avec la finalité envisagée

- **Exactitude et mise à jour**

  Être en mesure de gérer les modifications et les retraits

L'Analyse d'Impact relative à la Protection des Données (AIPD)

Permet d'évaluer le risque d'un traitement de données sur la vie privée des personnes concernées

- Obligatoire lorsque le traitement est susceptible d'engendrer des risques élevés
- Obligatoire si au moins deux des critères suivants sont remplis :

- Surveillance automatique,
- Données sensibles
- Collecte à grande échelle
- Croisement de données
- Personnes vulnérables (patients, personnes âgées, enfants, etc.)
- Evaluation/scoring (y compris profilage)
- Décision automatique avec effet légal
- Usage innovant ou utilisation NTIC
- Exclusion du bénéfice d'un droit, d'un contrat

La sécurisation des données (1)

- Pour garantir au regard des risques :
  - La **confidentialité** des données (données accessibles qu'aux personnes autorisées)
  - L'**intégrité** des données (données non altérées)
- A toutes les étapes du projet : collecte, échange, stockage…
- Incombe au responsable du traitement et au sous-traitant

Quelles **mesures** de sécurité ?

- **Physiques** (ex : sur les locaux, porte du bureau fermée, accès réservé aux serveurs)
- **Logiques** (ex : mot de passe individuel et robuste, antivirus mis à jour, verrouillage automatique, sauvegarde régulière, chiffrement des données)
- **Organisationnelles** (ex : charte informatique, gérer les habilitations des destinataires)
- **Sur les données** : anonymiser ou pseudonymiser les données le plus tôt possible

La sécurisation des données (2)

- Outils mis à disposition par l'Université de Poitiers
  - Collecte de données via un questionnaire en ligne : Limesurvey (proscrire Googleforms hébergé hors UE)
  - Stockage : serveurs UP (proscrire GoogleDrive, DropBox)
  - pour les échanges avec les parties prenantes : email professionnel (proscrire gmail)
  - pour les transferts de données : FileSender de Renater

- Autres solutions de stockage
  - Sharedocs de Huma-Num
  - MyCore du CNRS pour les UMR

L’anonymisation et la pseudonymisation des données

- **Pseudonymisation**

  Consiste à remplacer les données directement identifiantes par des données indirectement identifiantes (ex : numéro identifiant) → processus réversible

  - *Une table de correspondance est souvent mise en place*
  - *Chiffrer et cloisonner le fichier de correspondance*

- **Anonymisation**

  Rend impossible l’identification d’une personne → processus irréversible

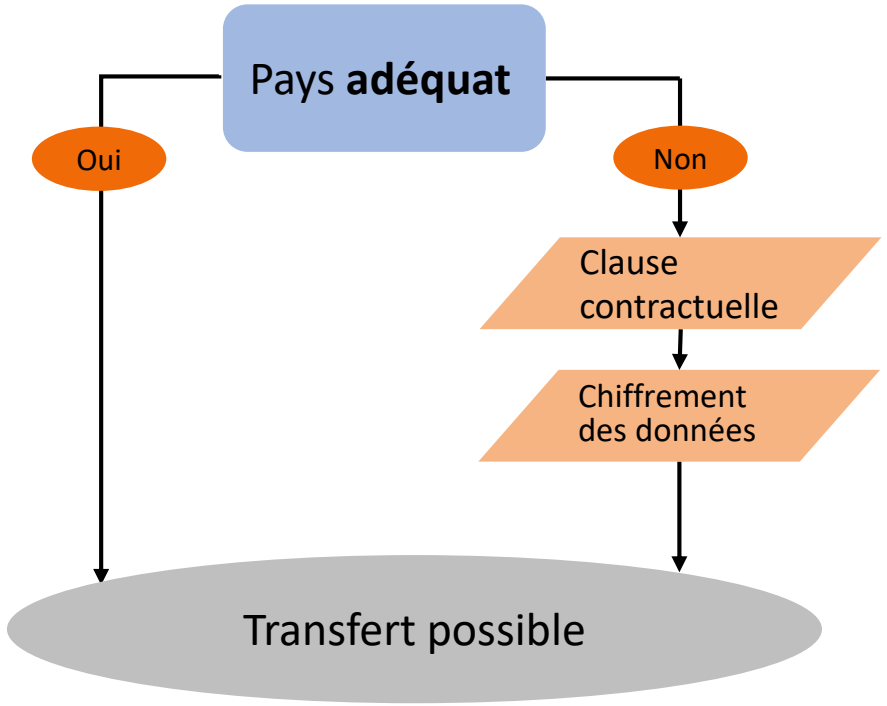
  - *Supprimer définitivement les données directement identifiantes*
  - *Minimiser les données indirectement identifiantes*
  - *Agréger les données de sorte à éviter toute individualisation*

  Objectif difficile à atteindre

Transfert des données

Le RGPD encadre les transferts de données hors Union Européenne afin d'assurer un niveau de protection des données suffisant et adapté.

La Cnil cartographie les différents niveaux de protection des données des pays dans le monde



Conservation des données

- Déterminée par la finalité du traitement
- **Prédéfinie et limitée**

A l'issue du traitement,

- Anonymisation
- Concernant la recherche :
  - Conservation possible pour une réutilisation ultérieure des données
  - Archivage possible selon des dispositions spécifiques

La transparence

→ Obligation d'informer les personnes des caractéristiques du traitement les concernant et de la manière d'exercer leurs droits

Quand?

Juste avant la collecte, dès la proposition de participer

Si modification importante du traitement (finalités, destinataires, problème de sécurité)

Informations qui doivent figurer dans la notice d'information :

- Identité et coordonnées du responsable du traitement
- Finalités
- Base légale
- Destinataires des données
- Durée de conservation
- Transfert des données hors UE
- Droits des personnes
- Coordonnées du DPO et de la Cnil

Droits des personnes

Les personnes bénéficient de nombreux droits qui leur permettent de garder la maîtrise de leurs données.

Leurs droits :

- Information
- Accès aux données
- Rectification et effacement
- Limitation du traitement
- Portabilité des données (sauf si mission d'intérêt public)
- Opposition
- Ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé

Elles peuvent exercer leurs droits auprès du responsable du traitement ou du DPO et en dernier recours auprès de la Cnil.

Le responsable du traitement dispose d'un délai d'un mois pour répondre à une demande.

Quelles démarches effectuer à l'UP ?

Quand?
Avant la mise en œuvre d'un traitement de données personnelles, le plus en amont possible du projet

- Renseigner la fiche de registre de traitement
- S'appuyer sur le **guide de mise en conformité** du DPO

- Échanges avec le DPO à son initiative afin d'éclaircir la demande de déclaration (souvent plusieurs allers-retours)
- Joindre la notice d'information et le cas échéant, le questionnaire, le formulaire de consentement ou de non-opposition

- Validation de la demande : le DPO attribue un numéro de traitement
- Le traitement est inscrit au **registre interne des activités de traitement de l'Université de Poitiers**

- Mise en œuvre du traitement dans les conditions annoncées
- Le cas échéant, ouvrir un compte LimeSurvey pour collecter les données en ligne

Pour aller plus loin

- Guide RGPD de l'InSHS
- Doranum, rubrique Aspects juridiques et éthiques
  - RGPD – Protection des données personnelles et RGPD dans la recherche : conséquences, obligations, implications
  - Webinaire des tuto@mate « Le RGPD appliqué aux SHS »
- Le RGPD à l'Université de Poitiers
- Le RGPD au CNRS (intranet)
- La Cnil
  - L'atelier RGPD de la Cnil
  - Le règlement RGPD

Merci pour votre attention

gaelle.coz@univ-poitiers.fr