LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Déléguée à la protection des données

dpo@univ-rouen.fr

Introduction

De la LIL au RGPD

Avant le 25 mai 2018

- Application de la **loi Informatique et libertés (LIL)** et d'une **directive européenne de 1995**
- **Déclarations auprès de la CNIL**
- Désignation facultative d'un **Correspondant Informatique et Libertés** dans l'établissement

Depuis le 25 mai 2018

- Application du **Règlement général sur la protection des données (RGPD)** et de la loi Informatique et libertés
- Suppression de la plupart des déclarations CNIL, remplacées par le **principe d'accountability**
- Désignation obligatoire d'un **Délégué à la protection des données** dans l'établissement

Les objectifs du RGPD

Protéger

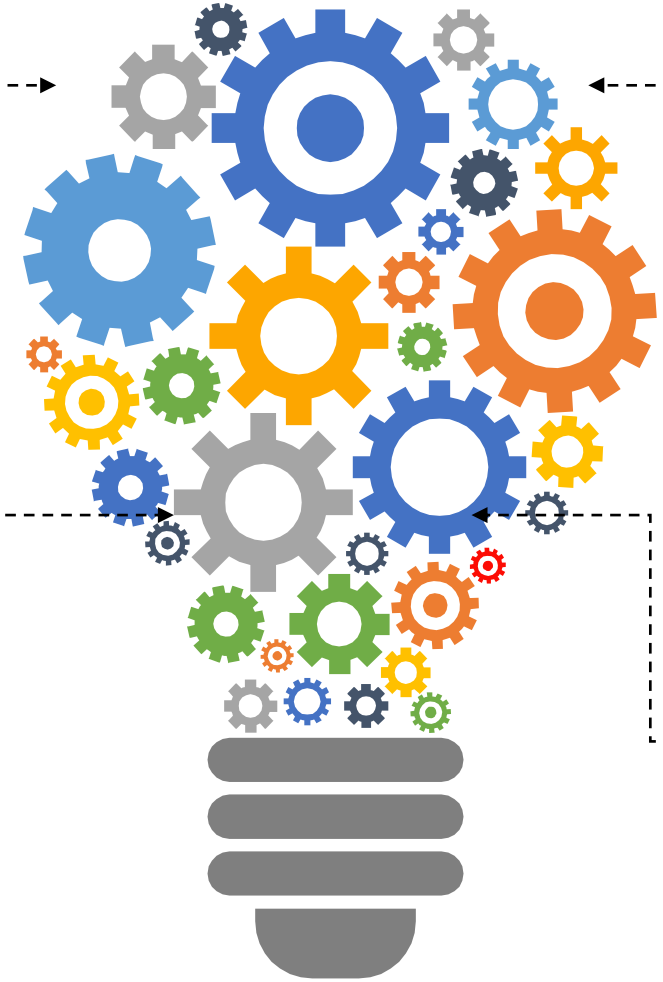
Protège la vie privée en **encadrant** les traitements de données à caractère personnel

Harmoniser

Uniformise les règles applicables sur le territoire de l'Union européenne

Sanctionner

Renforce les sanctions en cas de non-conformité afin de crédibiliser la protection des données personnelles



Renforcer

Renforce les droits des personnes sur leurs données personnelles

Responsabiliser

Dynamise le rôle du responsable du traitement dans le processus de mise en conformité

Rassurer

Tranquillise les usagers quant à l'utilisation qui est faite de leurs données personnelles

Les acteurs du RGPD

Responsable du traitement (RT) et Responsable conjoint du traitement	Sous-traitant (ST)	Personne concernée	Destinataires
• Détermine les finalités et les moyens du traitement, seul ou conjointement avec un autre RT	• Met en œuvre le traitement de données personnelles au nom et pour le compte du RT • Sa responsabilité peut également être engagée	• Personne dont les données sont traitées	• Toute personne qui reçoit communication des données • Et qui n'est ni RT, ni ST, ni personne concernée

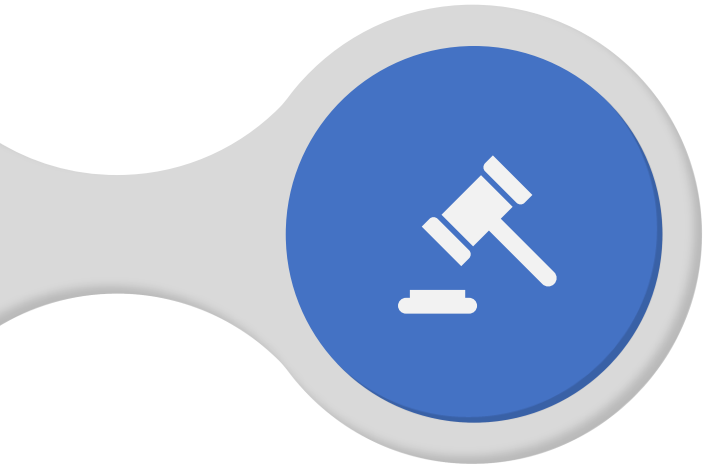
<u>En pratique, quel que soit le type de recherche :</u>

➔ Le **président de l'Université et le directeur d'unité** (pour les UMR) sont responsables pour l'unité de recherche que celle-ci agisse en tant que RT ou ST.

➔ Le **porteur du projet**, le responsable scientifique, est en charge des démarches administratives.

➔ Le **promoteur de la recherche** est en général responsable du traitement.

Risques encourus

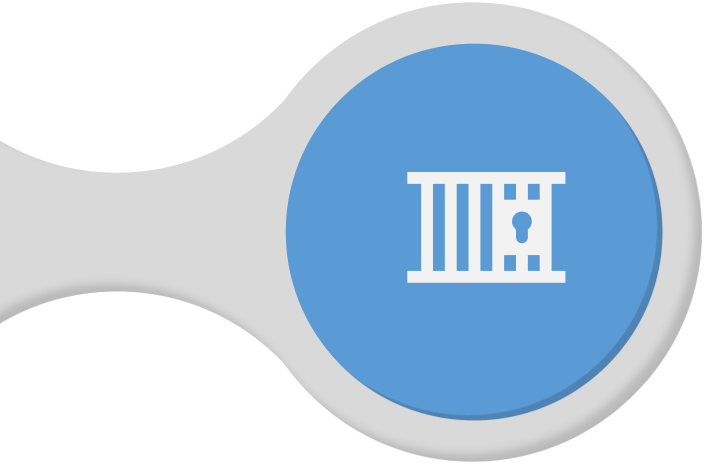


CONTRÔLE CNIL

- Avertissement
- Rappel à l'ordre
- Suspension du traitement
- Amende administrative : 10 à 20 millions d'euros

RÉPARATION

Réparation du préjudice subi par la personne : paiement de dommages et intérêts



SANCTION PÉNALE

Jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende (Art. 226-16 à 226-24 du Code penal)

RÉPUTATION

Impact négatif sur l'image et la réputation de l'organisme

Application du RGPD

Application du RGPD

Le RGPD s'applique :

- Aux traitements de données à caractère personnel

Que le traitement soit :

- Informatique ou papier

Pour les traitements :

- Mis en œuvre par des acteurs européens ou à destination des citoyens européens.

Qu'est-ce qu'une donnée personnelle ?

Toute information

Nom, âge, numéro d'identification, sexe, préférence alimentaire, marque de voiture, sport pratiqué, habitudes de vie, situation financière, allergies, métier,…

Identifié ou identifiable

Directement (*nom et prénom*) ou indirectement (*pseudonyme, fonction*), à partir d'une donnée (*ADN, NIR*) ou d'un recoupement d'informations (*l'étudiant en fauteuil roulant qui soutient sa thèse de médecine générale le 5 octobre à l'Université de Rouen*)

Portant sur un être humain

Les données relatives à une entreprise ou à un organisme ne sont pas concernées.

⚠ l'adresse mail professionnelle, le numéro de téléphone professionnel, la fonction,… sont des données personnelles de l'individu

Traitement de données à caractère personnel

Traitement :

Toute opération ou ensemble d'opérations portant sur des données à caractère personnel

Données sensibles (art. 9 du RGPD)

→ Principe :
Traitement interdit

→ Exceptions :
Traitement autorisé à des fins de recherche scientifique ou historique ou à des fins statistiques, si des garanties appropriées sont apportées (art.89 du RGPD)

Donnée anonyme ou pseudonyme ?

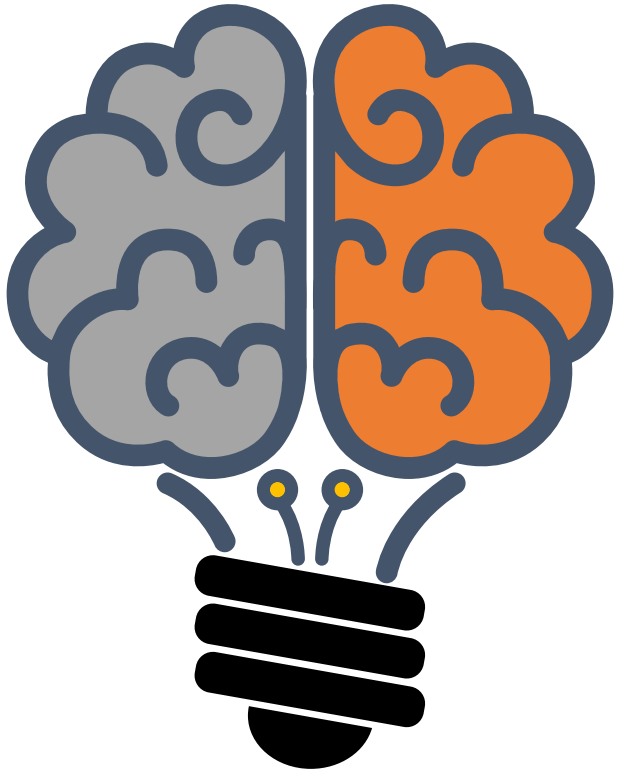
Donnée anonyme

➔**Toute ré-identification de la personne concernée est impossible**.

On ne peut ni individualiser, ni corréler, ni inférer.

L'anonymat est très rarement atteint.

S'il est atteint, il faut être en mesure de le démontrer.



Donnée pseudonyme

➔ **Les données directement identifiantes** (nom, prénom, adresse,…) **sont supprimées**. **Les données ne peuvent plus être directement attribuées à une personne concernée précise.**

Toutefois, par recoupement de plusieurs informations (âge, sexe, ville, diplôme,…), par le recours à des informations supplémentaires ou par l'utilisation de moyens techniques divers, il est possible d'identifier la personne.

Principe de précaution : en cas de doute, il faut toujours considérer que la donnée est pseudonyme et que le RGPD s'applique.

Principes RGPD

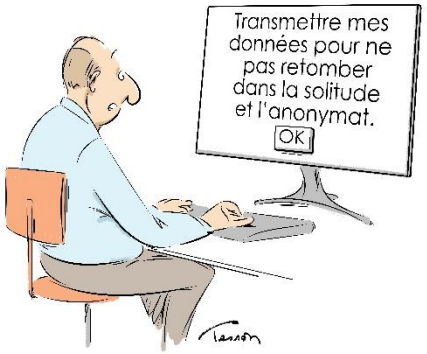
Principe 1 : Licéité, loyauté et transparence (art. 5 du RGPD)

Licéité

➔ Base légale du traitement, deux possibilités :

❑ **Consentement : libre, éclairé, spécifique et univoque**

Exemple
- à éviter s'il conduit à recueillir des données personnelles supplémentaires (nom, signature…)
- peut être retenu si d'autres consentements sont déjà recueillis



AFCDP
Le consentement doit être libre.

Attention à distinguer:
- consentement **au traitement des données à caractère personnel**
- consentement **à participer à la recherche**
- consentement **à l'enregistrement audio et/ou vidéo**

❑ **Mission d'intérêt public** : recherche scientifique et technologique, diffusion et valorisation de ses résultats (Art. L123-3 Code de l'éducation)

Exemple
- à privilégier pour des recherches où il n'est plus possible de contacter les personnes
- à éviter pour des recherches particulièrement risquées

>> La base légale est à adapter au cas par cas, ce travail est à considérer en lien avec le DPO <<

Principe 1 : Licéité, loyauté et transparence (art. 5 du RGPD)

Licéité

➔ Autres composantes de la licéité :

- ❑ **Déterminer le fondement du traitement des données sensibles**
- ❑ **Conclure une convention cadrant la relation entre RT et ST, ou entre co-RT**
- ❑ **Encadrer les transferts hors Union européenne, s'ils ne peuvent être évités**
- ❑ **Formaliser la conformité aux réglementations dans une documentation (acountability)**

Principe 1 : Licéité, loyauté et transparence (art. 5 du RGPD)

Loyauté et transparence

➔ Obligation d'informer les personnes concernées sur la façon dont seront utilisées leurs données et sur leurs droits

- **Au plus tard au moment du recueil des données :**

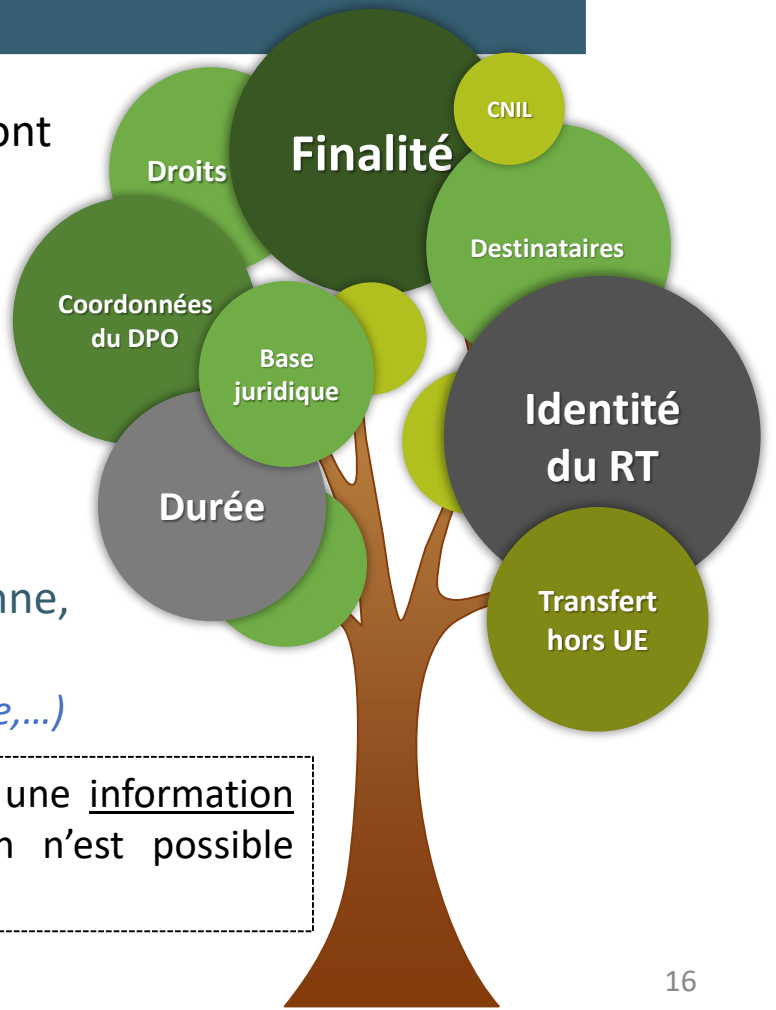
Si elles sont recueillies directement auprès de la personne et spécifiquement pour le traitement envisagé

Ex : questionnaire, entretien,…

- **Au plus tard un mois après le recueil des données :**

Si elles n'ont pas été recueillies directement auprès de la personne, ou ont été recueillies auprès d'elle pour une autre finalité.

Ex : réutilisation de données, extraction d'une BDD, utilisation d'un annuaire,…)



⚠ Si cette information demande **des efforts disproportionnés ou est impossible**, une information générale doit être envisagée *(affichage, site internet,…)*. Si aucune information n'est possible (individuelle ou générale), il faudra **être en mesure de le justifier.**

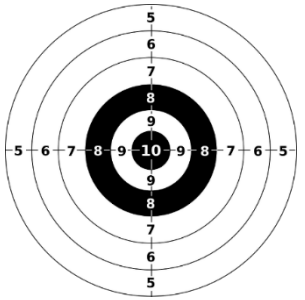
Droits à respecter

- Droit d'accès aux données
- Droit à la suppression des données
- Droit de rectification des données
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit d'opposition au traitement
- Droit de définir des directives relatives au sort des données après sa mort LIL

Principe 2 : Limitation des finalités (art. 5 du RGPD)

Limitation des finalités (art. 5 RGPD)

Les objectifs poursuivis par le traitement sont déterminés, explicites et légitimes. Ils justifient la nécessité d'utiliser des données personnelles.



Des traitements ultérieurs sont possibles **à des fins statistiques ou à des fins de recherche scientifique ou historique :**

- En apportant des garanties pour protéger la vie privée des personnes
- En informant les personnes concernées de ces nouvelles finalités.
- En déclarant ces nouvelles finalités au DPO.

Principe 3 : Minimisation des données (art. 5 du RGPD)

Minimisation des données

Les données sont adéquates, pertinentes et nécessaires

En pratique :

- ➔ **On ne traite pas de données simplement « au cas où »**
- ➔ On traite uniquement les données **nécessaires** au regard des finalités déterminées
- ➔ Des données supplémentaires pourront toujours être collectées plus tard
- ➔ Les zones de libre commentaire sont à éviter ou à encadrer strictement, les données collectées doivent être vérifiées (suppression des données inutiles)

Exemples

- l'âge des personnes est nécessaire à la recherche X mais leur date de naissance précise importe peu
- la région d'exercice de professionnels de santé est utile à la recherche Y mais l'adresse précise de leur cabinet ne présente aucun intérêt
- il est nécessaire de savoir si la personne exerce un métier manuel ou intellectuel, mais sa profession exacte n'a aucune incidence sur la recherche Z

Principe 4 : Limitation de la conservation (art. 5 du RGPD)

Limitation de la conservation

Limitation de la durée de conservation **à ce qui est nécessaire pour atteindre la ou les finalités.**

En pratique :

- Les durées sont déterminées au cas par cas (sauf obligation légale)
- Il peut s'agir d'une durée chiffrée (*5 ans*) ou de critères de détermination de la durée (*conservation des données jusqu'à la publication d'un article relatif à la recherche Y*)
- A l'issue du délai, les données doivent être anonymisées ou détruites
- Il est possible, dans le cadre de la recherche, de conserver les données en archives intermédiaires après ce délai :
  - ❑ En informant les personnes
  - ❑ En déclarant la conservation des données au DPO
  - ❑ En déterminant cette durée de conservation supplémentaire

Principe 5 : Intégrité et confidentialité (art. 5 du RGPD)

Intégrité et confidentialité

Des mesures techniques et organisationnelles doivent garantir la sécurité des données contre les traitements non autorisés ou illicites, la perte ou les dégâts d'origine accidentelle.

>>> La DSI et le RSSI de l'Université peuvent vous accompagner sur ces questions <<<

En pratique, quel que soit le support, il s'agit de :

- **Respecter les règles de bonnes pratiques** : verrouiller son bureau, sa session d'ordinateur, ne pas communiquer ses mots de passe, éviter les supports amovibles…
- **Gérer les habilitations** : déterminer qui a besoin et peut accéder aux données
- **Recourir à des services internes** : Limesurvey de l'Université, drive de l'Université, espaces de stockage de l'Université, boîte mail universitaire…
- **Stocker sur les serveurs de l'Université ou chiffrer les dossiers conservés localement**
- **Privilégier les espaces de stockage partagés, le drive ou Filex pour l'envoi de documents**
- **Signaler les violations de données dans les plus brefs délais à l'adresse dpo@univ-rouen.fr**

Check-list RGPD

1. Déterminer la base juridique du traitement
2. Définir de manière claire et précise l'objectif poursuivi
3. Limiter les données traitées à celles strictement nécessaires au regard de cet objectif
4. Être vigilant quant aux données sensibles et aux transferts hors UE
5. Déterminer la durée de conservation nécessaire pour accomplir l'objectif
6. Prévoir le sort des données à l'issue de cette durée
7. Prendre des mesures de sécurité techniques et organisationnelles
8. Informer les personnes sur le traitement avant sa mise en œuvre

Démarches RGPD

Inscription au registre des activités de traitement

Inscription au registre des activités de traitement de l'Université

- Atteste de la conformité au RGPD
- **Tenue d'une documentation complète <u>obligatoire</u>** : joindre à la déclaration tout document justifiant le respect du RGPD.
- Doit être réalisée **<u>avant</u>** la mise en œuvre du traitement
- S'obtient en contactant le DPO de l'unité
- **L'inscription doit être mise à jour en cas de changement dans le traitement**

<u>Contenu du formulaire de déclaration</u>

- Contexte, finalités du traitement et date de recueil
- Personnes concernées par le traitement
- Type de données traitées (recueillies, exploitées,…)
- Destinataires des données et transferts hors UE
- Recueil du consentement/Autre base légale
- Information des personnes
- Durée de conservation des données
- Mesures de sécurité

Analyse d'impact sur la protection des données

Réalisation d'une analyse d'impact sur la vie privée (AIPD)

- **Obligatoire pour les traitements présentant des risques élevés pour les droits et libertés des personnes.**

- **Objectif** : envisager les scénarios présentant des risques juridiques et techniques, lister les mesures existantes, apprécier le niveau de gravité et de vraisemblance de ces risques et déterminer les actions et les mesures à mener pour réduire ces niveaux

Exemples

Traitement figurant sur la liste noire de la CNIL :

- Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.)
- Traitements de données de localisation à large échelle

Exemples

Ou traitement répondant à deux des neufs critères de la CNIL :

- Données sensibles
- Collecte à large échelle
- Personnes vulnérables (patients, personnes âgées, enfants,…)
- Croisement de données

Exemples

Risques : accès illégitime, modification non désirée, disparition de données

Impacts : Discrimination, menaces, perte d'emploi, phishing,…

Mesures : minimisation des données, contrôle d'accès, chiffrement, traçabilité,…

LIENS UTILES

Liens utiles

- Niveau de protection des pays dans le monde (transferts hors UE) :
  https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
- Guide du CNRS pour les recherches en SHS :
  https://www.inshs.cnrs.fr/sites/institut_inshs/files/pdf/guide-rgpd_2.pdf
- Guide de la CNIL sur l'open data :
  https://www.cnil.fr/sites/default/files/atoms/files/guide_open_data.pdf
  https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data
- Analyse d'impact sur la vie privée (AIPD):
  https://www.cnil.fr/sites/default/files/atoms/files/171002_fiche_risque_fr_cmjk.pdf
  https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
  NB : Il y a également en bas de cette page un renvoi vers quatre documents qui détaillent le fonctionnement d'une AIPD mais ce ne sont pas des lectures rapides
- Liste des traitements nécessitant de réaliser une AIPD :
  https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf
- Critères pour effectuer une AIPD :
  https://www.cnil.fr/sites/default/files/atoms/files/infographie_aipd.pdf
- Recommandation du réseau des DPO de l'enseignement supérieur :
  https://reseau.supdpo.fr/wp-content/uploads/2020/01/SupDPO-Recommandations-chercheurs-v1.pdf
- Page de la CNIL relative au cadre de la recherche médicale :
  https://www.cnil.fr/fr/recherche-medicale-quel-est-le-cadre-legal