Déléguée à la protection des données

Les fondamentaux de la protection des données à caractère personnel

Formation doctorants 2022

Héloïse Faivre, DPO mutualisée

Université Grenoble Alpes, Université Savoie Mont Blanc, Grenoble INP et Sciences Po Grenoble

Déléguée à la protection des données

Définitions

Définition «données à caractère personnel»

- RGPD (art. 4.1) « on entend par **«*données à caractère personnel», 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* »

Déléguée à la protection des données

Données personnelles sensibles

- Données sensibles (art. 9 RGPD – art. 6 Loi I&L)
  - « *données à caractère personnel susceptibles de révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique,* ***des données concernant la santé*** *ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* »

Traitement à des fins de recherche possible, mais nécessitant la réalisation analyse d'impact sur la vie privée avec le DPO

Données de santé

Déléguée à la protection des données

- Données de santé : à partir de quand et jusqu'où ?
  - La notion de données de santé est **définie de manière large par le RGPD**
    - (RGPD consid. 35) *Les données à caractère personnel concernant* ***la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée****. […*
    - (RGPD art. 4.15) *«données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale 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*;
  - Collecte de données : des modes opératoires divers
    - recueil direct auprès de la personne (oral, questionnaire…)
    - mesures sur la personne : EEG, ECG, volume respiratoire…
    - inférence : possibilité de déduire de nouvelles informations relatives à la personne (calcul, recoupement de données…)

      ex. taille + poids → IMC = donnée de santé

  → à apprécier au cas par cas compte tenu de la nature des données collectées et traitées → avec le DPO

Autres définitions

Déléguée à la protection des données

- **Traitement** : toute(s) opération(s) automatisée(s) ou non effectuée(s) sur des données à caractère personnel depuis leur collecte jusqu'à leur effacement
- **Personne concernée** : la personne physique à laquelle se rapportent les données collectées et traitées
  - **ex**. participant.e(s) à une recherche (et investigateurs) ; membres du laboratoire...
- **Destinataire(s)** : toute(s) personne(s) ou groupe de personnes ou organisme à qui sont communiquées des données à caractère personnel
  - **ex. traitements administratifs** → tutelles, HCERES…
  - **ex**. **traitements de recherche** → mise à disposition de données de recherche

- **Pseudonymisation** : mesures appliquées à des données à caractère personnel de telle façon qu'une personne **physique ne puisse être identifiable par ses données sans avoir recours à des informations supplémentaires** […] conservées **séparément** et soumises à des mesures garantissant l'impossibilité d'identifier cette personne
  - ex. en recherche : table de correspondance : [identité du volontaire / numéro anonyme]
    données de recherche : [numéro anonyme + données personnelles non identifiantes]

Déléguée à la protection des données

Les principales lois applicables

- le **Règlement général sur la protection des données (RGPD)**
  - RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
  - **application uniforme dans l'UE depuis le 25 mai 2018**

- la **Loi Informatique et Libertés** [**RGPD + SECTEURS SANTÉ, POLICE/JUSTICE**]
  - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée

Déléguée à la protection des données

Que dit la Loi ?

5 Principes fondamentaux à respecter

Déléguée à la protection des données

1. les **finalités** du traitement : objectifs de la collecte (directe ou non) de données personnelles

   → licites, déterminées, explicites et légitimes

2. la **minimisation** et la **pertinence** des données

   → nécessaires aux finalités et non excessives

3. **durée de conservation des données limitée**

   → limitée à la durée strictement nécessaire aux finalités

4. **sécurité** (pérennité, intégrité) **et confidentialité** des données

   → proportionnée aux finalités et aux données traitées

5. **respect des droits** des personnes :

   → **information**, accès, opposition, suppression, retrait…

Licéité (art. 6 du RGPD)
« Ai-je le droit de mettre en œuvre ce traitement ? »

Déléguée à la protection des données

→ au moins une des 6 bases légales

1. **consentement libre et éclairé des personnes**

   →après information règlementaire complète, claire, concise, adaptée aux personnes

   →pratique courante en recherche impliquant des personnes

2. exécution d'un **contrat** auquel la personne concernée est partie
3. **obligation légale** à laquelle le responsable du traitement est soumis
4. **intérêt vital** de personnes physiques (personne concernée ou autre personne physique)
5. **exécution d'une mission d'intérêt public**

   → base légale des traitements de recherche

6. **intérêt légitime** du responsable de traitement

Les principes du RGPD à respecter pour la mise en œuvre d'un traitement

Déléguée à la protection des données

- **responsabilité et preuve de conformité**

le responsable de traitement doit être en mesure de prouver la conformité à tout instant

  - → registre des traitements du laboratoire + documentation des traitements (ex. dossiers CERGA)

- **minimisation des données collectées**

- **protection des données de bout en bout d'un projet** (*privacy by design*)

Les principes du RGPD à respecter pour la mise en œuvre d'un traitement

Déléguée à la protection des données

- **protection des données par défaut** (*privacy by default*) : organisation, pratiques, outils… au quotidien
  - → **sécuriser l'ordinateur** du chercheur (outil recommandé : VeraCrypt)
  - → **chiffrer** les enregistrements, les photos (trombinoscopes), les données confidentielles ou sensibles…
  - → **ne pas communiquer par pièce jointe à un mail** les fichiers de données personnelles
    - → **utiliser un service sécurisé de dépôt/téléchargement** (ex. FileSender de RENATER)
- **analyse d'impact relative à la protection des données** (AIPD)
  - pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques

Quelques points de vigilance

Déléguée à la protection des données

- **droit à l'image, droit à la voix**
  - **La collecte, la conservation, l'utilisation de photos (trombinoscopes) ou d'enregistrements vidéo ou audio sont soumises au consentement <u>exprès</u> (autorisation) de la personne**
- **minimisation des données collectées**
  - → ex. collecter une tranche d'âge ou un âge et non la date de naissance
  - → ex. utiliser des listes fermées (inclusion…) → question : « êtes-vous concerné.e par au moins un item ? »
- **attention aux données implicites (risque d'identification par recoupement avec d'autres données de la recherche)**
  - **<u>ex1</u>**. étude sur enfants de ***l'école maternelle xxxxx de Grenoble*** *+ collecte* **profession parents**

Quelques points de vigilance

Déléguée à la protection des données

- Anonymisation vs pseudonymisation

  - anonymisation → identification directe ou indirecte **impossible**
  - pseudonymisation → identification impossible **sans information supplémentaire**

- Outils numériques : attention aux plates-formes gratuites "grand public" !
  - Privilégier les outils ou infras internes (GRICAD, MSH…)
  - Privilégier les outils qui relèvent du droit européen

Déléguée à la protection des données

En recherche

lien entre éthique et protection des données personnelles

Sources sur l'éthique

- *Fédération des Comités d'éthique pour les recherches (FCER)*
- *Comité d'éthique pour la recherche, Grenoble Alpes (CERGA) [Carole Peyrin]*

2 domaines **distincts mais fortement liés**

Déléguée à la protection des données

Éthique en recherche (sur et avec des personnes physiques)

- Respect des principes universels de dignité humaine et primauté de l'être humain
  - Intérêt public
  - Bienfaisance dans les objectifs et la démarche : « balance bénéfices/risques »
  - Autonomie et libre arbitre des participants
  - → consentement libre et éclairé
  - Justice, équité et impartialité
  - Rigueur et intégrité scientifique
- Cadres réglementaires ou contraignants
  - Code de Nuremberg (1946)
  - Déclaration d'Helsinki (1964)
  - Santé : Loi du 5 mars 2012 relative aux recherches impliquant la personne humaine (« loi Jardé ») → Code de la santé publique

Protection des données personnelles en recherche

- Respect des droits et libertés et de la vie privée des personnes physiques
  - Licéité (intérêt public)
  - Légitimité et proportionnalité
  - loyauté
  - Information, consentement ou opposition, limitation…
  - Conformité légale
- Cadres réglementaires
  - RGPD (2016)
  - Loi informatique et libertés (1978)
  - Santé : Loi du 5 mars 2012 relative aux recherches impliquant la personne humaine (« loi Jardé ») → Code de la santé publique

Déléguée à la protection des données

Pour approfondir

Site de la CNIL (très riche !)
www.cnil.fr

Règlement général sur la protection des données
https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

Loi Informatique et Libertés
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

Éthique et RGPD recherche (Fédération des CER et SupDPO)
https://pod.univ-lille.fr/ethique-et-protection-des-donnees-en-recherche/

Éthique (CERGA)
http://www.grenoblecognition.fr/index.php/ethique/ (rubrique ÉTHIQUE)

Déléguée à la protection des données

Merci de votre attention