

COMMENT CONCILIER PARTAGE ET PROTECTION DES DONNÉES DE RECHERCHE ?

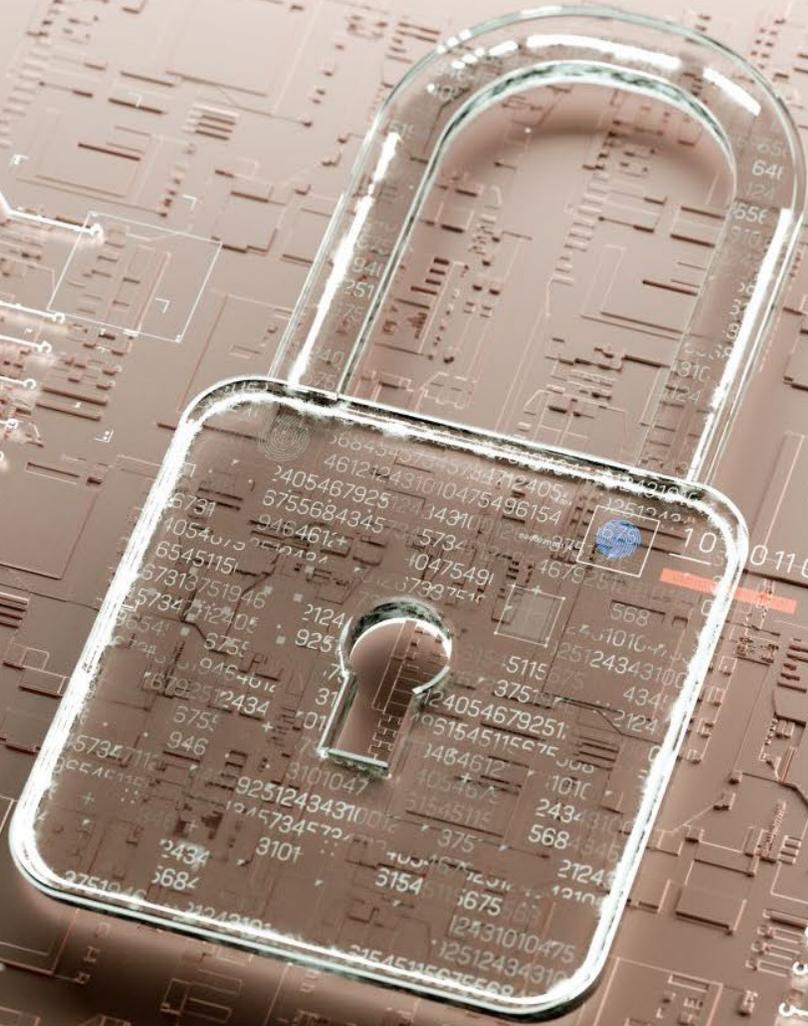
Chloé Gay-Balmaz

Webinaire

31 octobre 2023 > 12h15 – 13h30

Informations

- Ce webinaire sera enregistré puis publié sur les pages ORD (site internet HES-SO)
- Plage de 15 mn Q&A > 13h15 – 13h30
- Micros > OFF
- Webinaire le 27 février 2024 > Droit d'auteur et licences



Session
questions – réponses

Protection des données & Open Research Data

Chloé Gay-Balmaz
31 octobre 2023

- Les données issues d'une personne défunte sont-elles des données personnelles ? Sont-elles léguées à la famille ?
- Est-il nécessaire de recueillir le consentement de personnalités politiques pour analyser leurs propos publiés dans les médias ou les personnalités publiques ont-elles un statut spécifique ?
- Est-il nécessaire de recueillir le consentement d'individus pour étudier les propos qu'ils ont publié sur les réseaux sociaux ?
- Est-il permis d'utiliser des données personnelles issues d'archives publiques ?

Qu'est-ce qu'une donnée personnelle?

Données personnelles

(art. 5 lit. a LPD)

toutes les **informations**

concernant une **personne physique**

identifiée ou identifiable

Données personnelles et «vie publique»

En règle générale, il n'y a **pas atteinte à la personnalité** lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement.

(art. 30 al. 3 LPD)

Les **intérêts prépondérants du responsable du traitement** entrent notamment en considération [...lorsque...] les données personnelles recueillies concernent une personnalité publique et se réfèrent à son activité publique.

(art. 31 al. 2 lit. f LPD)

- Un chercheur détient-il la propriété intellectuelle de l'idée ?
- Y a-t-il des procédures standardisées pour l'anonymisation d'images, dans le cadre d'un projet de recherche portant sur un corpus d'œuvres picturales sous droit d'auteur ?
- Est-ce qu'il est nécessaire de requérir un droit de cession pour utiliser dans un projet de recherche des données générées par des étudiant·e·s ?
- Les données générées par les étudiant·e·s leur appartiennent-elles?
- Est-il nécessaire de requérir le consentement des étudiants pour la diffusion et l'utilisation de leurs travaux, appelés à être diffusés dans différents médias ?

Protection des données personnelles ou propriété intellectuelle?

Art. 15 de la Convention intercantonale sur la Haute Ecole Spécialisée de Suisse Occidentale (HES-SO)

1. Les hautes écoles sont titulaires des **droits de propriété intellectuelle** portant sur toutes les créations intellectuelles ainsi que les résultats de recherches obtenus dans l'exercice de leurs fonctions par les personnes ayant une relation contractuelle de travail avec ces dernières.

Les **droits d'auteur** ne sont pas concernés par cette disposition.

2. Les hautes écoles sont titulaires des droits d'utilisation exclusifs des **logiciels** que des personnes ayant des rapports de travail avec elles créent dans l'exercice de leur fonction. Les hautes écoles peuvent convenir avec les ayants droits de se faire céder les droits d'auteur sur les autres catégories d'œuvres.

3. Les hautes écoles assurent la protection et la valorisation des résultats de la recherche, notamment par des demandes de brevets et par leur exploitation commerciale directe ou l'octroi de licences. A défaut, dans un délai de 12 mois, les droits dont elles sont investies retournent aux personnes qui sont à l'origine des **créations** considérées.
4. Une **indemnité équitable** est versée à l'auteur de **l'invention** si l'exploitation de celle-ci engendre des bénéfices.
5. Les dispositions particulières prévues par les hautes écoles et les organes de financement de la recherche sont réservées.
6. Les droits sur les **biens immatériels** résultant de collaborations font l'objet de contrats spécifiques.

- Qui doit-être tenu pour responsable lorsqu'un jeu de données, anonymisées de façon imparfaite, est mis à disposition du public, sachant que le responsable de traitement est généralement le scientifique mais que les données appartiennent à l'institution à laquelle il est affilié ?
- L'institution peut-elle se retourner contre le chercheur en cas de litige ?
- Qui doit avoir accès aux consentements éclairés, lors du projet et lorsque le chercheur quitte l'institution?

Qui est responsable du traitement de données?

Responsable du traitement

Traitement de données personnelles

la personne privée ou publique qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens** du traitement de données personnelles (~ art. 5 lit. j LPD)

toute **opération relative à des données personnelles**, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (art. 5 lit. d LPD)

- Le personnel de recherche a l'habitude de maintenir des listes de contacts pour communiquer des résultats et événements relatifs à des projets de recherche ou des activités de l'institut: est-il encore permis d'avoir de telles listes et de les utiliser pour diffuser différentes informations et invitations par email?
- Combien de temps est-il permis de stocker des données personnelles?

À quelles conditions est-il possible de constituer et d'établir et de conserver une «liste de contacts»?

Principes de protection des données

¹ Tout traitement de données personnelles doit être **licite**.

² Il doit être conforme aux principes de la **bonne foi** et de la **proportionnalité**.

³ Les données personnelles ne peuvent être collectées que pour des **finalités déterminées et reconnaissables** pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités.

⁴ Elles sont **détruites ou anonymisées dès qu'elles ne sont plus nécessaires** au regard des finalités du traitement.

⁵ Celui qui traite des données personnelles doit s'assurer qu'elles sont **exactes**. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexacts ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées.

⁶ Lorsque le **consentement** de la personne concernée est requis, celle-ci ne consent valablement que si elle exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée.

⁷ Le consentement doit être **exprès** dans les cas suivants:

- a. il s'agit d'un traitement de données sensibles;
- b. il s'agit d'un profilage à risque élevé effectué par une personne privée;
- c. il s'agit d'un profilage effectué par un organe fédéral.

(art. 6 LPD)

Droits des personnes concernées

Droit de savoir

- Droit d'être informé
 - De tout traitement de données (art. 19 s. LPD)
 - En cas de décision individuelle automatisée (art. 21 LPD)
 - En cas de violation de la sécurité des données (art. 24 LPD)
- Droit d'accès (art. 25 ss LPD)
- Droit à la remise des données (art. 28 LPD)

Droit de s'opposer au traitement

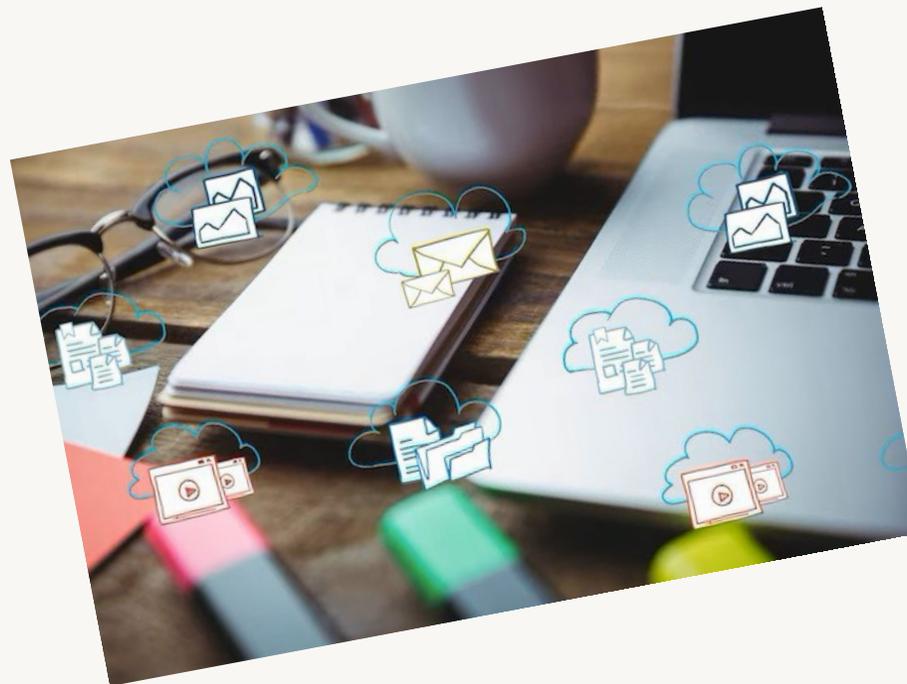
- Droit à l'autodétermination informationnelle (art. 10 al. 2 Cst. féd.)
- Droit de s'opposer au traitement
(art. 32 al. 2 lit. LPD, 28a CC et 41 al. 1 LPD)
- Droit de faire effacer et détruire des données
(art. 32 al. 2 lit. c LPD et 41 al. 2 lit. a LPD)
- Droit de faire rectifier des données inexactes
(art. 32 al. 1 lit. a ou b LPD et 41 al. 2 lit. a LPD)
- Droit de faire mentionner le caractère litigieux (art. 41 al. 5 LPD)

Obligations du responsable de traitement

- Informer (art. 19 ss LPD)
- Tenir un registre des activités de traitement (art. 12 LPD)
- Annonce les violations de la sécurité des données (art. 24 LPD)
- Effectuer une analyse d'impact (art. 22 LPD)

- Lors de la communication de données personnelles à l'étranger (art. 16 ss LPD)
- Lors d'une éventuelle sous-traitance (art. 9 LPD)

- Est-il permis de traiter des données sensibles?



Que sont les données personnelles sensibles et est-il permis de les traiter?

**Données
(personnelles)
sensibles**

1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales
2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique
3. les données génétiques
4. les données biométriques identifiant une personne physique de manière univoque
5. les données sur des poursuites ou sanctions pénales et administratives
6. les données sur des mesures d'aide sociale

Consentement exprès

(art. 6 al. 6 en lien avec 7 LPD)

- Faut-il respecter la Loi fédérale sur la protection des données en attendant que la Loi cantonale de protection des données soit révisée, notamment concernant certaines prescriptions fédérales plus sévères?

Quelle est la réglementation de protection des données personnelles applicable?



Responsable de
traitement affilié à la
HES-SO?

-> **Loi cantonale**

Collaboration ...

- en Suisse?
 - quelle est l'affiliation du (des) partenaire(s)?
 - HES-SO?
 - EPF?
 - institut ou entreprise privé(e)?
 - à des fins ne se rapportant pas à des personnes?
- à l'étranger?
 - dans l'UE?
 - hors de l'UE?

Recherche en santé? LRH

- Quelle réglementation s'applique lorsque les données traitées proviennent de citoyens européens ?
- Quelle réglementation s'applique lorsque le projet de recherche est mené sur territoire européen ?

Quand le Règlement Général européen sur la Protection des Données personnelles (RGPD) est-il applicable?

Applicabilité du **R**èglement **G**énéral européen sur la **P**rotection des **D**onnées personnelles (art. 3 al. 2 RGPD)

Principe de territorialité

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un **responsable du traitement ou d'un sous-traitant sur le territoire de l'Union**, que le traitement ait lieu ou non dans l'Union.

Exception

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des **personnes concernées qui se trouvent sur le territoire de l'Union** par un **responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union**, lorsque les activités de traitement sont liées:

- a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
- b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

- Quelles conditions dois-je respecter pour transférer des données personnelles à l'étranger, et en particulier hors de l'UE ?



Principe: **“Niveau de protection adéquat”**

(art. 16 al. 1 LPD)

“Niveau de protection approprié”

(art. 16 al. 2 LPD)

Dérogations: **Liste exhaustive**

(art. 17 LPD)

- Sur quels supports les données personnelles devraient-elles être stockées ?
- Sur quels supports les données personnelles ne devraient-elles surtout pas être stockées ?
- Quels risques y a-t-il à déposer son jeu de données sur une plateforme (data repository) américaine ?
- Par quels moyens techniques les données personnelles devraient-elles être partagées lorsque le projet intègre plusieurs partenaires de diverses institutions suisses ?

Comment concrètement stocker et partager des données personnelles?

**Crypter.
Crypter.
Et crypter.**

+

**MESURES
ORGANISATIONNELLES**

! «les bonnes pratiques» !

NB: Switch



- Comment bien choisir son outil d'anonymisation?
- Les outils d'anonymisation tels qu'Amnesia ou Qamydata sont-ils sûrs ?

Comment crypter les données?

Pas de «one size fits all»!

> **étudier les données traitées à la lumière de la finalité du projet**

> **demander conseil à un ingénieur**

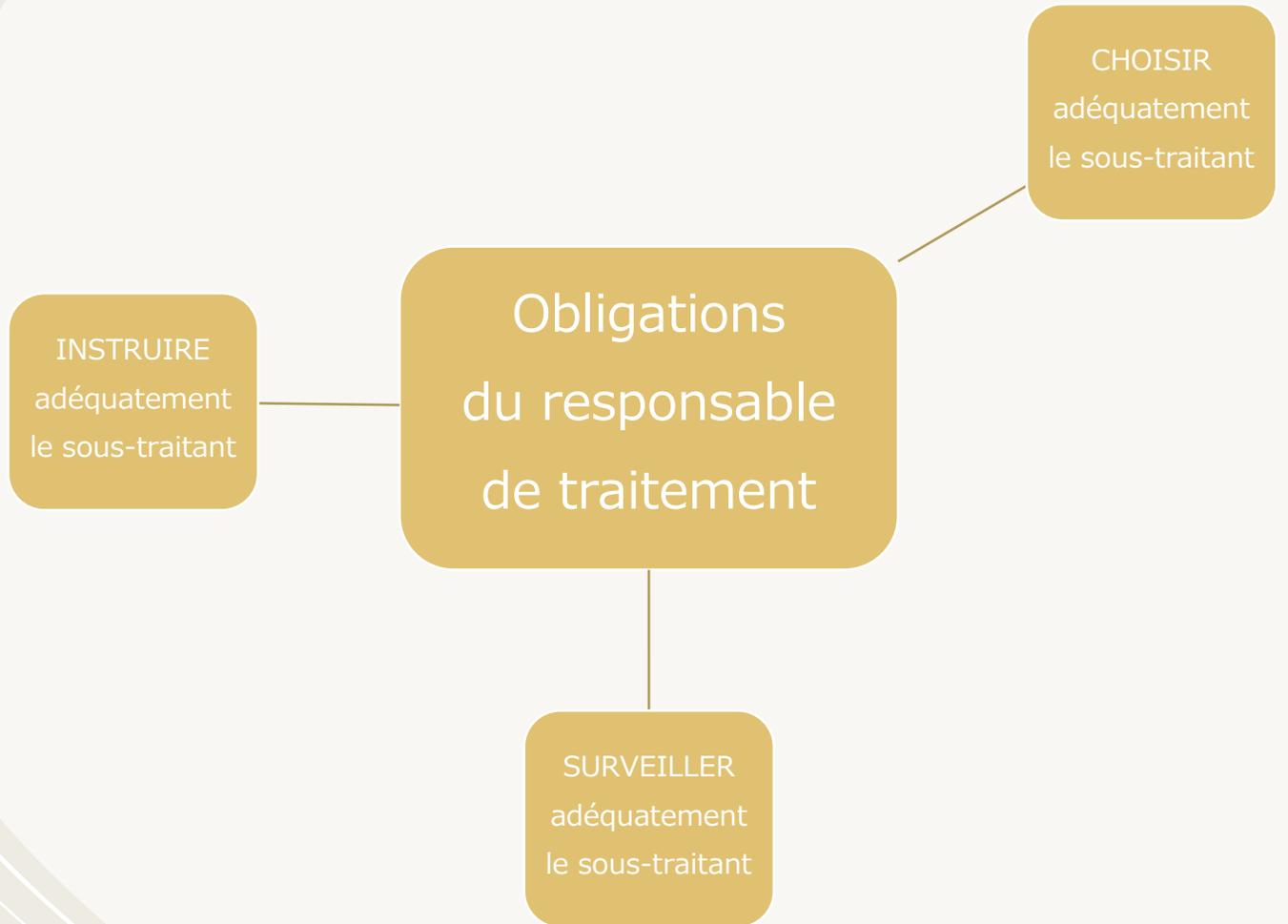


- Comment s'assurer que le sous-traitant respecte les bonnes pratiques en matière de sécurité ?
- Est-il nécessaire d'établir un contrat spécifique pour chaque projet de recherche entre un institut de recherche et un même sous-traitant ?

Comment contrôler un sous-traitant?

Par contrat.

Plus précisément,
par le registre des
activités de traitement.



- **A-t-on l'obligation de tenir un registre des traitements des données personnelles ?**

Oui.

Art. 12 Registre des activités de traitement

1. Les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement.
2. Le registre du responsable du traitement contient au moins les indications suivantes:
 - a. l'identité du responsable du traitement;
 - b. la finalité du traitement;
 - c. une description des catégories de personnes concernées et des catégories de données personnelles traitées;
 - d. les catégories de destinataires;
 - e. dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation;
 - f. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8;
 - g. en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues à l'art. 16, al. 2.
3. Le registre du sous-traitant contient des indications concernant l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement ainsi que les indications prévues à l'al. 2, let. f et g.
4. Les organes fédéraux déclarent leur registre d'activités de traitement au PFPDT.
5. Le Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.

- **Qu'est-ce qu'une analyse d'impact et comment la réaliser ?**

L'analyse d'impact contient:

- une description du traitement envisagé
- une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concerné
- les mesures prévues pour protéger sa personnalité et ses droits fondamentaux

**Une obligation
du responsable de traitement**

(art. 22 LPD)

- **Quelle est la sanction applicable au partage de données insuffisamment anonymisées ?**



Amende maximale de CHF 250'000.-



Questions complémentaires?