Hes·so

FAQ – PROTECTION DES DONNÉES PERSONNELLES (DANS LE CONTEXTE DE LA RECHERCHE ET DE L'OPEN RESEARCH DATA)

Document révisé par Franco Lorenzetti et Catherine Ingold-Schuler

Version octobre 2024

Notions fondamentales

1. Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à une physique identifiée ou identifiable. Par exemple, son adresse e-mail, son domicile, ses évaluations académiques.

2. Qu'est-ce qu'une donnée sensible ?

Une donnée sensible est une donnée personnelle particulièrement protégée, car elle concerne (la liste exhaustive figure à l'art. 14 CPDT-JUNE) :

a) Les opinions ou les activités religieuses, philosophiques, politiques ou syndicales;
b) La santé (anamnèse, diagnostic, prescription, etc.), la sphère intime, l'origine ou l'ethnie;
c) Les données biométriques et génétiques;
d) Les mesures d'aide sociale ou d'assistance;
e) Les poursuites ou sanctions pénales et administratives.

Législations applicables

3. En tant que chercheur.euse affilié.e à une haute école de la HES-SO, suis-je soumis·e à la Loi fédérale sur la protection des données?

La Loi fédérale sur la protection des données (LPD) s'applique aux personnes privées (personnes physiques et entreprises) et aux organes fédéraux. Elle ne s'applique donc pas aux hautes écoles publiques de la HES-SO qui sont des institutions cantonales, et à ce titre sont soumises à la législation cantonale sur la protection des données :

- GE : Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)
- FR : Loi sur la protection des données (LPrD)
- JU-NE : Convention intercantonale des 8 et 9 mai 2012 relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)

- VD : Loi sur la protection des données personnelles (LPrD)
- VS : Loi sur l'information du public, la protection des données et l'archivage (LIPDA)

Exemple : si un·e chercheur·euse est affilié·e à une des hautes écoles du canton de Genève, elle ou il sera soumis-e à la LIPAD.

Il convient de préciser que l'EHL, la manufacture et Changins, sont des institutions de droit privé, elles sont soumises à la LPD.

Dans certains projets européens, si la ou le responsable du projet est situé·e en Europe, le RGPD s'appliquera. Par conséquent, une institution se verra imposer les principes RGPD, même si la loi applicable est la loi cantonale.

4. Est-on soumis à 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 ?

Les lois cantonales révisées sont basées sur la LPD du 25 septembre 2020 et sur le RGPD. Pour les cantons n'ayant pas encore révisé leur loi de protection des données, c'est une bonne pratique d'appliquer les principes figurant dans la LPD ou dans le RGPD, même si la loi en vigueur reste applicable.

5. Lors de partenariat avec des instituts ou des entreprises privées, quelle loi prévaut ?

L'entreprise privée suisse sera soumise à la LPD. L'institution cantonale sera soumise à la loi cantonale de son siège. Il faudra déterminer qui des deux est la ou le responsable du traitement, et notamment si l'institution cantonale est un sous-traitant de l'entreprise privée ou un·e responsable du traitement.

6. Il y a-t-il un régime spécial pour les données de santé ?

La Loi relative à la recherche sur l'être humain (LRH) établit les principes fondamentaux qui doivent être observés dans les projets de recherche sur l'être humain. Elle s'applique en priorité, et au surplus c'est la législation idoine sur la protection des données qui s'applique. La LRH s'applique à la recherche sur les maladies humaines et sur la structure et le fonctionnement du corps humain (art. 2 al. 1 LRH). Les données de santé sont les informations concernant une personne déterminée ou déterminable qui ont un lien avec son état de santé ou sa maladie, données génétiques comprises (art. 3 let. f LRH).

Responsabilités

7. Qui est responsable du traitement des données ?

Selon Art. 14 let. f Convention JUNE sur la protection des données et la transparence des 8 et 9 mai 2012, la ou le responsable du traitement est « l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données ». Cette notion est reprise par d'autres lois cantonales. Par exemple, Art. 3 al. 6 de la LIPDA (Loi valaisanne sur l'information du public, la protection des données et l'archivage du 9 octobre 2008) précise que la ou le responsable du traitement est : « l'autorité, le service ou tout autre organisme public ou privé qui, seul ou conjointement avec d'autres, dans l'accomplissement de ses tâches légales, détermine les finalités et les moyens du traitement de données personnelles.»

En d'autres termes, c'est l'institution qui sera généralement la responsable du traitement au sens juridique. Dans le cas par exemple d'une violation des données, ce sera l'institution qui assumera la responsabilité juridique. Cependant, l'institution délèguera aux scientifiques toutes les tâches de la ou du responsable du traitement. Cette délégation pourra être décrite par exemple dans une politique interne de protection des données. Notons par ailleurs que la notion de propriété intellectuelle des données n'intervient pas dans la responsabilité.

8. Il y a des obligations spéciales de la ou du responsable de traitement lorsque les données personnelles sont communiquées à l'étranger ou lors d'une éventuelle sous-traitance des données ?

On parle de sous-traitance lorsque l'entreprise principale (responsable du traitement) fait réaliser par une entreprise tierce tout ou partie des travaux ou services qu'elle s'est engagée à fournir à ses clients. La ou le responsable du traitement ne peut pas se décharger de sa responsabilité sur le sous-traitant : elle ou il doit notamment s'assurer que celle-ci ou celui-ci respecte la sécurité des données. Certaines législations cantonales exigent un contrat de sous-traitance, ce qui reste une bonne pratique. Si on envisage de communiquer des données personnelles à l'étranger, il faut s'assurer que le pays est en adéquation selon l'annexe 1 de l'OPDo.

9. Est-ce que plusieurs personnes peuvent-être responsable du traitement ? IT, archivistes ? chercheur.euse ?

Si plusieurs responsables du traitement décident ensemble de la finalité du traitement et des moyens mis en œuvre, on peut parler de responsables conjoints du traitement. Dans les autres cas, on aura un·e seul·e responsable du traitement, qui devra s'assurer que tous les principes de protection des données sont respectés, notamment la sécurité de l'information assurée par les équipes IT. Le responsable de traitement est l'institution. Celle-ci délègue des compétences en matière de traitement aux collaborateur·trices, qui sont des responsables de traitement délégués. L'archivage constitue un traitement spécifique. Si l'archivage est une des opérations dans le cadre de la recherche, on pourra considérer que la ou le chercheur·euse en est le responsable du traitement délégué. S'il s'agit en revanche d'un processus global au sein d'une institution, un archiviste pourra en être la ou le responsable du traitement délégué.

10. Comment s'assurer que la ou le sous-traitant·e respecte les bonnes pratiques en matière de sécurité ? Est-il nécessaire d'établir un contrat spécifique pour chaque projet de recherche entre le sous-traitant et votre institution ?

L'établissement d'un contrat de sous-traitance est une bonne pratique. Certaines législations cantonales l'imposent. Ce contrat permet d'exiger notamment que la ou le sous-traitant·e mette en place des mesures de sécurité et qu'il ne traite pas les données confiées autrement que ce qui est convenu.

11. Est-ce que la chercheuse ou le chercheur a l'obligation de tenir un registre des activités de traitement des données personnelles ?

Le registre des activités de traitement est une obligation légale qui va dépendre de la loi applicable, et notamment du canton dans lequel se trouve l'établissement. Certaines lois cantonales imposent la tenue du registre des activités de traitement qui consiste à recenser tous les traitements de données personnelles. S'il existe un·e DPO (Data protection Officer ou délégué à la protection des données), c'est généralement elle ou lui qui se chargera de

consolider les informations fournies par le·la chercheur·euse dans le registre. Tout cela relève de l'organisation interne de l'établissement (responsable du traitement) en matière de protection des données. Le·la chercheur·euse devra fournir les informations concernant le traitement qu'il effectuera avec son projet. On pourra généralement définir que chaque projet traitant des données personnelles correspond à un traitement.

Collecte des données

12. Peut-on collecter des données personnelles accessibles publiquement ?

En règle générale, il n'y a pas d'atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun. Toutefois, il s'agit de s'assurer qu'elle ne s'est pas opposée expressément au traitement. Il faudra analyser le but dans lequel les données personnelles avaient été mises à disposition publiquement et s'assurer que la nouvelle utilisation prévue soit compatible avec ce but. De manière générale, il faudra renoncer aux traitements auxquels les personnes ne pouvaient raisonnablement pas s'attendre ou alors demander leur consentement.

13. Est-ce que les données d'une personne défunte sont encore des données personnelles ?

En droit suisse, la personnalité et donc sa protection s'éteint avec la mort de la personne.
La LPD ne s'applique donc pas aux données d'une personne décédée.

14. Puis-je librement collecter et traiter des données personnelles d'une personnalité publique ?

Malgré les différents comportements qui peuvent constituer des atteintes à la personnalité, il y a divers motifs justificatifs de ces atteintes. Cela veut dire que pour certains motifs, la licéité peut être levée. C'est par exemple le cas de cet article 31 al. 2 let. f LPD, les intérêts prépondérants de la ou du responsable du traitement entrent notamment en considération lorsque les données personnelles recueillies concernent une personnalité publique et se réfèrent à son activité publique. Il faudra mettre en balance l'intérêt de la ou du responsable de traitement avec la protection de la personne concernée.

15. Est-il permis d'utiliser des données personnelles issues d'archives publiques ?

On pourra partir du principe que les personnes concernées ont donné leur consentement pour la publication dans les archives publiques, ou alors qu'il s'agit d'une obligation légale. On peut réutiliser ces données, ce qui constituera un nouveau traitement pour lequel il faudra respecter les principes de protection des données.

16. Le consentement est-il toujours requis ?

Le consentement n'est pas toujours requis. C'est un motif justificatif qui permet notamment de justifier une atteinte illicite à la personnalité.

Sécurité des données

17. Comment sécuriser ses données de recherche ?

Idéalement, il faudrait anonymiser les données dès que possible. Comme l'anonymisation est souvent synonyme de perte de valeur des données pour la ou le chercheur·euse, on lui préférera la pseudonymisation. Celle-ci consiste à remplacer les données identifiantes par un code et stocker la correspondance entre code et données identifiantes dans une table de correspondance bien protégée et accessible à peu de personnes. Il existe de multiples possibilités de sécuriser les données personnelles. On citera notamment le chiffrement symétrique ou asymétrique.

18. Qui doit avoir accès au consentement éclairé lors du projet et lorsque la chercheuse ou le chercheur quitte l'institution ?

Lorsque le consentement de la personne concernée est requis, celle-ci doit pouvoir s'exprimer librement et après avoir été informée. Un consentement exprès (exprimé clairement et de façon non équivoque, oralement ou par écrit) est exigé lorsqu'on traite des données sensibles ou que l'on fait du profilage à risque élevé. Si un consentement est demandé, la personne concernée devra également pouvoir le retirer. La forme écrite ou électronique du consentement s'impose donc afin de permettre ce suivi du consentement. Une personne concernée devra donc pouvoir retirer son consentement et il faudra mettre en œuvre un processus qui permettra de gérer cette demande même si le chercheur a quitté l'institution. D'un point de vue juridique, la responsabilité de gérer ce consentement incombera à l'institution.

Stockage, archivage des données

19. Combien de temps est-il permis de stocker des données personnelles ?

Le stockage est un terme assez vague et il mérite d'être mieux défini :

- Stockage : opération consistant à enregistrer des données sur un support (disque dur, clé USB, …)
- Sauvegarde : opération consistant à effectuer une copie de sécurité des données à un instant t. L'opération inverse est la restauration. En anglais : backup and restore.
- Archivage : à la fin de la période d'utilisation des données, opération consistant à déplacer les données dans une archive. Les archivistes parlent d'archivage intermédiaire (lié à la durée de conservation) et d'archivage définitif (sans limitation dans le temps).

La durée de conservation est le temps pendant lequel on peut ou on doit conserver les données. Cette durée de conservation est définie d'une part par d'éventuelles obligations légales (p. ex. 10 ans pour la comptabilité ou 20 ans pour les dossiers médicaux) et d'autre part, par la ou le responsable du traitement. Les données ne peuvent être conservées que pendant le temps nécessaire à réaliser la finalité déterminée au début du traitement.

Transfert/Partage des données

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

La LPD comme les lois cantonales mentionnent des dispositions spécifiques pour la communication (transfert) de données à l'étranger. En principe, les données personnelles ne peuvent être transmises à l'étranger que si le pays destinataire assure un niveau de protection des données adéquat. L'annexe 1 de l'OPDo donne une liste des Etats en adéquation. Si tel est le cas, il s'agit de chiffrer ses données à l'aide d'un outil de chiffrement pour le tramsfert.