Questionnaires

Définitions et conseils

1431 Université de Poitiers

"Des savoirs & des talents"

Qu'est-ce que le RGPD ?

Le sigle RGPD signifie *« Règlement Général sur la Protection des Données »* (en anglais *« General Data Protection Regulation »* ou GDPR).

Il est entré en vigueur le 25 mai 2018. Il s'inscrit dans la continuité de la Loi française Informatique et Libertés (LIL) de 1978.

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

3 OBJECTIFS

- **Mieux protéger les données personnelles des citoyens**
- **Harmoniser la protection des données au niveau de l'Europe**
- **Responsabiliser l'ensemble des acteurs du secteur privé et public et les citoyens**

Université de Poitiers

Définitions

Traitement : Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition.

Destinataire : La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Finalité du traitement : Il s'agit de l'objectif principal de l'utilisation de données personnelles.

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 »* de manière directe ou indirecte.
- Art. 4 du RGPD

Exemples de données personnelles relatives à une personne physique :

- Nom, prénom, pseudonyme, date de naissance ;
- Photos, enregistrements audios et vidéos, signature ;
- Numéro de téléphone fixe ou portable, adresse postale, adresse e-mail ;
- Adresse IP, identifiant de connexion informatique ou identifiant de cookie …

Les **données de contact** des personnes (adresse e-mail), les **données d'inclusion**, les **données implicites** (lieu de l'étude) et les **données socio-démographiques** sont considérées comme des données personnelles. Elle doivent être prises en compte pour évaluer le risque d'identification des personnes.

Il ne s'agit donc pas uniquement de données « confidentielles » ou relative à la vie privée des individus, mais bien de **toute information ayant un pouvoir d'identification**.

La collecte porte-elle sur des données sensibles ?

Données sensibles

Données qui révèlent :

- L'origine raciale ou ethnique ;
- L'orientation ou la vie sexuelle ;
- Les opinions politiques ou appartenance syndicale ;
- Les convictions philosophiques ou religieuses ;
- Des données génétiques ou biométriques ;
- Des données en lien avec la santé (numéro de sécurité sociale, port de lunettes…) ;
- Des données de condamnation pénale (LIL);
- Numéro NIR .

Il est **interdit de recueillir et d'utiliser des données sensibles**, sauf dans certains cas précis, encadrés et définis notamment à l'art. 9.2 du RGPD :

- Si la personne concernée a donné son consentement exprès (écrit, clair et explicite) ;
- Si ces données sont nécessaires et justifiées par l'intérêt public pour la recherche dans le domaine de la santé.

Il est donc possible de recueillir des données sensibles dans certains cas,
mais à condition d'accomplir impérativement les formalités adéquates
(Par exemple, mettre en œuvre une MR en cas d'étude en santé)

Qu'est-ce qu'une donnée de santé ?

Certaines données personnelles sont considérées comme particulièrement sensibles : c'est le cas, entre autres, des données de santé d'une personne.

Selon la CNIL, *« les données à caractère personnel concernant la santé 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 »*.

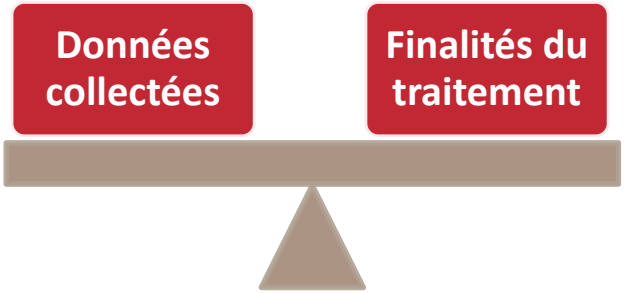
Trois catégories de données de santé :

- Les données de santé « par nature » : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- Les données de santé « par croisement » : du fait de leur croisement avec d'autres données, elles deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne ; croisement d'une mesure de poids avec la taille ce qui permet de calculer l'IMC (= donnée de santé), croisement de la tension avec la mesure de l'effort, etc.
- Les données de santé « par destination » : ce sont les données qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Principe de minimisation des données

*« Les données à caractère personnel doivent être : […] **adéquates**, **pertinentes** et **limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ; »*
- Art. 5.1(c) du RGPD

Le principe de minimisation est donc une obligation légale qui fait écho au principe de proportionnalité déjà présent au sein de la Loi informatique et liberté de 1978. Il s'applique désormais à toute personne qui collecte et opère un traitement de données.
↳ Exemple : collecter une tranche d'âge, plutôt que l'âge exacte.



L'investigateur ne doit traiter que les données personnelles strictement nécessaires pour atteindre l'objectif initial.

L'anonymisation – RGPD ou non ?

Avantages : l'anonymisation permet :

→ De garantir la confidentialité des données, la protection des droits et libertés du participant et le respect de sa vie privée.

→ **De sortir du cadre du RGPD**.

Pour aider à évaluer une bonne solution d'anonymisation, le G29 propose trois critères :

- ❑ L'individualisation : est-il toujours possible d'isoler un individu ?
- ❑ La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- ❑ L'inférence : peut-on déduire de l'information sur un individu ?

Ainsi, un ensemble de données pour lequel il n'est possible ni d'individualiser, ni de corréler, ni d'inférer est *a priori* anonyme.

Remarque : Bien sûr, il n'est **pas obligatoire de rendre le processus d'une enquête anonyme**, rien ne l'impose.
Un enquête **non anonyme** n'est pas mauvaise pour autant (Se méfier des idées reçues)..

Anonymisation vs pseudonymisation

Anonymisation	Pseudonymisation
Processus irréversible	Processus réversible
L'**anonymisation** est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible. Il existe deux principales techniques : ▪ **Randomisation** : transformer les données pour qu'elles ne se réfèrent plus à une personne déterminée. ▪ **Généralisation** : généraliser les données de façon qu'elles ne soient plus spécifiques à un individu, mais communes à un ensemble de personne.	La **pseudonymisation** permet de traiter les données à caractère personnel d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, numéro séquentiel, etc.).

Quel processus de sécurité mettre en place pour sécuriser les données collectées ?

Le RGPD impose une obligation de sécurisation des données et toute fuite ou atteinte à l'intégrité des systèmes engage la responsabilité du responsable de traitement, et d'éventuelles sanctions.

- → En cas de violation de données, la DPO doit être informée immédiatement pour aider à effectuer les démarches obligatoires vis-à-vis de la CNIL.
- → Lorsque les fuites comportent des risques pour les personnes, il peut être nécessaire d'informer nominativement les personnes concernées.
- → Outre les cas de piratage, le simple fait de perdre un ordinateur ou une clé USB contenant des données personnelles constitue un manquement à l'obligation de sécurisation.

Dès lors, il est important d'adopter de bonnes pratiques en matière de sécurité informatique :

- ❑ Sécuriser l'ordinateur de l'investigateur (mots de passe robustes / « pare-feu » / antivirus …)
- ❑ Chiffrer les enregistrements, les photos, les données sensibles (VeraCrypt) …
- ❑ Transfert de fichiers contenant des données sensibles par serveur de dépôt (Renater FileSender)
- ❑ Utiliser la messagerie de l'Université de Poitiers
- ❑ Utiliser des outils sécurisés pour les visioconférences (WebEx)
- ❑ Utiliser des outils sécurisés pour réaliser des enquêtes en ligne (LimeSurvey)
- ❑ Eviter d'utiliser un cloud « made in GAFAM » – préférer RESANA

Pour plus d'information, consultez le guide de la CNIL« Sécurité des données personnelles ».

Respecter les droits des personnes concernées

Le RGPD reconnaît aux personnes concernées par un traitement de données à caractère personnel une série de droits sur leurs données qu'elles peuvent exercer et que les responsables de traitement doivent être en mesure de respecter :

- Droit à l'information : toute personne doit être prévenue que des données la concernant sont traitées et informée, notamment, des finalités poursuivies par ce traitement. Ces informations doivent lui être communiquées préalablement à la collecte, de manière claire et concise.
- Droits d'accès et de rectification : toute personne peut demander à un responsable de traitement la communication des données la concernant et exiger leur modification en cas d'erreur.
- Droits d'opposition et à l'effacement : toute personne peut – à condition que le cadre légal choisi le permette - s'opposer à un traitement de données pour faire cesser le traitement et demander à ce que les informations la concernant soient détruites (droit à l'oubli).
- Droit à la portabilité des données : toute personne peut – à condition que le cadre légal choisi le permette - demander à un responsable de traitement que lui soit remise les données la concernant dans un format structuré, couramment utilisé et lisible par machine (ordinateur) afin qu'elle puisse les réutiliser (Peu utilisé en recherche).

L'information

Responsable du traitement :

L'Université de Poitiers, représentée par Mme la Présidente, 15 rue de l'Hôtel Dieu TSA 71117 86000 Poitiers

Base légale du traitement (article 6.1.e RGPD) : Mission d'intérêt public

Finalités du traitement :

-Mesurer les cognitions sociales des élèves en fonction des activités scolaires présentées

-Enregistrer (audio) l'entretien pour garantir l'exactitude des réponses fournies

-Production de publications anonymes

Déléguée à la protection des données (DPO) : Pascal Martin (dpo@univ-poitiers.fr)

Destinataires des données (toute personne amenée à manipuler les données) : Equipe de recherche

Durée de conservation des données :

- Les données sont conservées en base active jusqu'à deux ans après la dernière publication des résultats de la recherche ou, en cas d'absence de publication, jusqu'à la signature du rapport final de la recherche puis archivées pendant une durée de 15 ans.
- L'enregistrement audio sera détruit après la fiabilisation des réponses

Droits sur vos données à caractère personnel

Vous disposez du droit d'accès, de rectification, à l'effacement, de limitation du traitement et d'opposition.
Vous pouvez exercer vos droits auprès du responsable scientifique de la recherche xxxxxxxxx(xxxxxxxxxxx@univ-poitiers.fr) ou auprès du délégué à la protection des données à l'adresse dpo@univ-poitiers.fr.
Si la réponse apportée demeurait insatisfaisante, il est possible d'adresser une réclamation à la Commission nationale de l'informatique et des libertés (CNIL) :
3 place de Fontenoy
TSA 80715
74334 Paris Cedex 07
www.cnil.fr

Conseils - questionnaire

- Favoriser l'utilisation d'un outil conforme RGPD – L'UP a choisi **LimeSurvey** – Parfois **SPHINX**.
- Le questionnaire est-il **anonyme** : oui/non.
- Si non, il doit :
    - Faire l'objet **d'une déclaration** auprès du DPO;
    - Comporter **une information RGPD conforme article 13 du RGPD** en tête;
    - Être mis en œuvre de telle sorte que les **personnes** doivent pouvoir exercer **leurs droits** ;
    - Être traité de manière **sécurisée**;
    - Avoir un **délai de conservation** en adéquation avec la finalité poursuivie.
- Le questionnaire comporte des données **directement identifiantes** (Nom, prénom, mail) : oui/non;
- Si **non** : Prévoir d'inclure **un pseudonyme** pour faciliter l'exercice des droits;
- Le questionnaire comporte des **données sensibles** : oui/non
- Si **oui** : Le traitement de la donnée sensible ne se fait qu'avec **un consentement** libre, éclairé et univoque de la personne;
- Le questionnaire est dans le **domaine de la santé** avec des **données de santé**: oui/non;
- Si **oui** : ⚠ Prendre contact avec le **DPO** avant toute démarche;
- **IMPORTANT :** Pendant la durée de conservation des données, la personne peut-elle **facilement exercer ses droits ?**

Prise de contact DPO

- Question au DPO :
https://rgpd.appli.univ-poitiers.fr/plugins/formcreator/front/formdisplay.php?id=1

- Effectuer une pré-déclaration de traitement en ligne :
https://survey.appli.univ-poitiers.fr/679477?lang=fr

- Demande d'ouverture de compte LimeSurvey :
https://glpi.appli.univ-poitiers.fr/plugins/formcreator/front/formdisplay.php?id=23

Qu'est-ce qu'une AIPD?

Lorsque le traitement des données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, la réalisation d'une analyse d'impact relative à la protection des données – AIPD (en anglais, *« privacy impact assessment »* ou PIA) est demandée. Elle permet d'évaluer ce risque.

- **Mise en œuvre** : l'analyse est réalisée par le responsable du traitement (et par délégation, l'investigateur) en lien avec le DPO et le responsable de la sécurité des systèmes d'information.

- **Quand est-ce qu'une analyse d'impact est obligatoire ?**

  → Soit le traitement de données envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une AIPD (cf. Délibération n° 2018-327 du 11 octobre 2018 : impose la mise en place d'une AIPD en cas de collecte de données sensibles).

  → Soit le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29 :

  - Surveillance automatique,
  - Données sensibles,
  - Traitement 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 DPO peut décider la nécessité de recourir à une AIPD même si les critères ne sont pas réunis. Elle évalue les risques pour l'établissement (RT)

Université de Poitiers

Références numériques

CNIL : https://www.cnil.fr/

LIL : https://www.cnil.fr/fr/la-loi-informatique-et-libertes

RGPD : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Contacts

Pascal Martin (DPO)
Direction générale - Université de Poitiers
15 rue de l'Hôtel Dieu
86 000 Poitiers
05-49-36-60-05
dpo@univ-poitiers.fr

© Université de Poitiers 2023 – Tous droits réservés