Les changements induits par le RGPD pour les chercheurs

Direction du **numérique** | DNUM
Université de Strasbourg

Déléguée à la protection des données

Auteur : Sarah Piquette-Muramatsu dpo@unistra.fr

Sommaire

1 . Concepts-clés

Définitions

Traitement

Toute opération appliquée à des données à caractère personnel (de la collecte jusqu'à l'archivage)

Délégué à la protection des données

Chargé de la mise en oeuvre de la conformité dans l'établissement qui l'a désigné

Responsable de traitement

La personne physique ou morale qui détermine les finalités et les moyens du traitement

→ le président de l'université ou le directeur de l'unité de recherche en co-tutelle

1. Concepts-clés

Donnée à caractère personnel :

« *Toute information identifiant directement ou indirectement une personne physique* »

→ **directement** : n°INE, ADN, nom et prénom…

→ **indirectement** : combinaison du quartier de résidence, de l'âge, du sexe et de la pratique sportive…

Article 4§1 RGPD

Exemple d'enquête

Les données suivantes sont collectées auprès des enquêtés :

- Profession
- Âge
- Genre
- Lieu d'exercice de la profession
- Niveau d'études

Cette enquête est-elle anonyme?

2. Formalités

RGPD = suppression de la plupart des formalités

→ Vérification de la conformité du traitement désormais assurée par le responsable du traitement

→ Prise de contact nécessaire du **délégué à la protection des données** avant une recherche impliquant des données personnelles

→ Réalisation d'une **Analyse d'impact sur la protection des données**

→ Création de nouveaux cadres de **recherche dans le domaine de la santé**, parfois applicables aux SHS

Contacts : dpo@unistra.fr / dpd.demandes@cnrs.fr / dpo@inserm.fr

2. Formalités

RGPD = suppression de la plupart des formalités

Analyse d'impact sur la protection des données = envisager les impacts du traitement sur la vie privée des personnes participant à la recherche.

→ le traitement de leurs données leur fait –il courir un risque immédiat ou à long terme? (*harcèlement*, *exclusion d'un droit*, *licenciement*…)

→ quels impacts en cas d'accès à ces données par des personnes non autorisées? En cas de disparition des données?…

Un outil dédié : PIA

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

2. Formalités

Diffusion des données

Vigilance concernant ce qui sera rendu public, notamment via un site internet :

- Consentement des personnes
- Limitation des données identifiantes

3. Les différentes catégories de données

Données bénéficiant d'une protection particulière: (Art9 §1 RGPD)

Données qui révèlent:

- Origine raciale ou ethnique
- Opinions politiques
- Convictions philosophiques ou religieuses
- Appartenance syndicale

Ainsi que:

- Données de santé,
- Vie et orientation sexuelle,
- Données génétiques,
- Biométriques (permettant d'identifier une personne de manière unique)
- et celles relatives aux condamnations pénales et aux infractions ainsi qu'aux mesures de sûreté connexes

Principe: interdiction de les traiter.

3. Les différentes catégories de données

EXCEPTIONS

→ **L'objectif de la démarche** : fins archivistiques dans l'intérêt public, recherche scientifique ou historique, statistiques

→ Le **consentement explicite** de la personne concernée

→ La **nature de la structure** : association, fondation, organisme à but non lucratif

→ Données **manifestement rendues publiques** par la personne concernée

4. La base légale du traitement

- **Consentement de la personne**
- Exécution d'un contrat
- Respect d'une obligation légale
- Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
- **Mission d'intérêt public**
- Intérêts légitimes du responsable de traitement

4. La base légale du traitement

1 Le consentement

- Pour la participation à un évènement
- Pour l'inscription à une newsletter

Conditions :

- Preuve du consentement explicite et éclairé
- Droit du retrait du consentement :

  Remise en question de la légalité du traitement mais uniquement pour l'avenir : les données déjà acquises le restent.

- Autorisation nécessaire du titulaire de la responsabilité pour les mineurs de moins de 15 ans

4. La base légale du traitement

1 Le consentement

Attention le consentement peut également être recueilli mais pas en tant que base légale:

- Consentement éclairé (informed consent)
- Accord pour la publication de données ou de l'image de la personne concernée

2. La mission d'intérêt public

Pour la recherche scientifique.

5. Principes fondamentaux de la protection des données

Une réflexion permanente :

- Pourquoi ?
- Quoi ?
- Pendant combien de temps ?
- Par qui ?
- Comment ?
- Quelle information des personnes ?

5. Principes fondamentaux de la protection des données

Pourquoi ? : Finalités du traitement

Les finalités du traitement doivent être :

- Déterminées
- Explicites
- Légitimes

→ Exposer la problématique de la recherche et\ou l'utilisation qui sera faite des données

→ Réutilisation des données possible si compatibilité avec les finalités d'origine.

Exception : réutilisation à des « *fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques*»

5. Principes fondamentaux de la protection des données

Quoi ? : Proportionnalité et pertinence des données

Les données collectées doivent être :

- Pertinentes
- Adéquates
- Limitées par rapport aux finalités

→ Déterminer pourquoi on a besoin des ces données

- À quoi vont- elles servir ?
- Sont-elles vraiment nécessaires pour atteindre l'objectif ?

5. Principes fondamentaux de la protection des données

Quoi ? : Proportionnalité et pertinence des données

Exemples:

- Participation à un évènement: nom, prénom, adresse mail et ?
- Envoi d'une newsletter: adresse mail et c'est tout!

Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.(C39)

5. Principes fondamentaux de la protection des données

Pendant combien de temps? (conservation limitée)

❖ Détermination nécessaire de la durée de conservation des données :

→ Prévoir la période pendant laquelle il sera indispensable d'accéder aux données afin de mener à bien la recherche , la gestion de l'évènement…

→ Prévoir le sort des données par la suite (destruction, archivage…)

Exemple :

- Gestion d'un évènement : conservation des données 1 mois après l'inscription
- Gestion d'un abonnement à une newsletter : jusqu'à désabonnement par la personne concernée

5. Principes fondamentaux de la protection des données

Comment ? (mesures de sécurité)

❖ Nécessité d'envisager les mesures de sécurité pour chaque étape du traitement :

→ Mode de **collecte** : papier, questionnaire en ligne sécurisé…

→ **Hébergement** des données : endroit, niveau de sécurité…

→ **Communication** interne à l'équipe : quels moyens de transmission?

→ **Sauvegarde** : quels supports ?

Exemples :

- Chiffrement des dossiers contenants les données
- Cloisonnement des bases de données pour éviter la ré-identification par recoupement

5. Principes fondamentaux de la protection des données

Comment ? (mesures de sécurité)

- Nécessité de vérifier si les solutions techniques fournies par des prestataires extérieurs respectent ces principes.

Exemple :

- Une application d'enquête en ligne, la société éditrice assure-t-elle elle-même l'hébergement des données?
  - Si oui, où? En France, dans l'UE, ailleurs?
  - Si non, à quelle société d'hébergement fait-elle appel? Celle-ci héberge-t-elle les données en France, dans l'UE, ailleurs?

5. Principes fondamentaux de la protection des données

Vigilance concernant les services gratuits

→ google forms, dropbox, gmail, onedrive, iCloud, Amazon Cloud Drive…

❖ Exemples des conditions d'utilisation **Microsoft** :

« *(…) vous* ***accordez à Microsoft une licence*** *de propriété intellectuelle internationale à titre gratuit* ***pour utiliser Votre Contenu*** *et, par exemple, le copier, le conserver, le transmettre, modifier son format, le diffuser via des outils de communications et l'afficher sur les Services.* »

5. Principes fondamentaux de la protection des données

Vigilance concernant les services gratuits

❖ Exemples des conditions d'utilisation **Google**:

« Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, ***vous accordez à Google*** *(et à toute personne travaillant avec Google)* ***une licence****, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'oeuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution*

publique desdits contenus. »

5. Principes fondamentaux de la protection des données

Choix des moyens informatiques (liste non exhaustive)

❖ **Collecte des données**

– LimeSurvey : hébergement via les serveurs de l'Université

– Evento : géré et hébergé par Renater, suppression des données au bout de 6 mois

❖ **Pour la communication**

– Messagerie Unistra

– Listes de diffusion Sympa

❖ **Pour le stockage ou partage des données**

– Seafile / ODS MyCore : création de bibliothèques chiffrées

– Moodle

– Gestion électronique des documents (GED)

5. Principes fondamentaux de la protection des données

Information des personnes

Obligation de loyauté et de transparence dans le traitement

→ Droits des personnes

- Droit d'accès aux données
- Droit de rectification
- ...

→ Mentions particulières

- Durée de conservation des données
- Responsable du traitement
- Contact du DPO

→ Collecte indirecte des données

- Mentions spécifiques

4. Principes fondamentaux de la protection des données

Information des personnes :

Exemple :

« Les informations recueillies le sont pour les besoins d'une thèse en..... À l'Université de Strasbourg. Elles seront traitées par ..... Elles seront conservées ..... Vous disposez de droits d'accès et de rectification sur vos données. Pour les exercer, veuillez adresser votre demande à.....

Vous pouvez également contacter la déléguée à la protection des données de l'université de Strasbourg à l'adresse suivante : dpo@unistra.fr »

6. Cas concrets

- **Collecte des données via un questionnaire/ formulaire en ligne :**

  → choisir un outil adéquat et protecteur des données

  → le respect des principes de finalité et de minimisation des données guidera l'élaboration des questions

  Exemples :

  - la date de naissance (JJ/MM/AA) est-elle indispensable? Ou des tranches d'âge peuvent –elles suffire?
  - L'adresse ou bien un département?

  → prévoir les mentions d'information avant la collecte des données (page d'accueil du questionnaire)

  → prévoir un espace dédié pour le recueil du consentement, si celui-ci est nécessaire

6. Cas concrets

- **Hébergement, stockage des données** :

  → un ordinateur personnel /un ordinateur fourni par le laboratoire, l'établissement?

  → accès aux données après authentification? Dans un dossier chiffré? Sur un support amovible (disque dur externe, clé usb…)

  → un « cloud » proposé par l'université, le laboratoire? Une solution grand public?

  → pérennité du stockage?

Idem pour les données collectées sur support papier : où les fiches de recueil du consentement des participants, questionnaires seront-ils stockées? Chez l'investigateur, au sein du laboratoire ou dans les locaux de l'équipe de recherche?

6. Cas concrets

- Communication via des listes de diffusion

Principe:

- Information
- Droit d'opposition

Lorsque l'on veut envoyer une information groupée à différents destinataires avec lesquels un contact préalable n'a pas été établi, il convient d'informer pourquoi ils reçoivent ce message et leur laisser la possibilité de s'opposer à recevoir d'autres mails de notre part.

Cas particulier des données de santé

Données de santé = 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.

Selon les objectifs de la recherche et la méthodologie envisagée la recherche peut entrer dans le cadre de la « loi Jardé » ou non, ce qui a un impact sur les démarches et formalités à effectuer.

Merci de votre attention

Pour me contacter: dpo@unistra.fr