Intervention à GEODE, UMR CNRS 5602

La protection des données personnelles dans les projets de recherche

→ 01/03/2024

Sommaire

01

Pourquoi protéger les données personnelles ?

Pourquoi protéger les données personnelles ?

Article 8 de la Charte européenne des droits fondamentaux

- Les données sont la propriété de chacun
- Importance de respecter la vie privée et les données

Le respect des objectifs des tutelles des unités

√ **Conduire notre mission de recherche publique**

√ **Pratiques éthiques de la recherche : Code de la recherche, décret de décembre 2021**

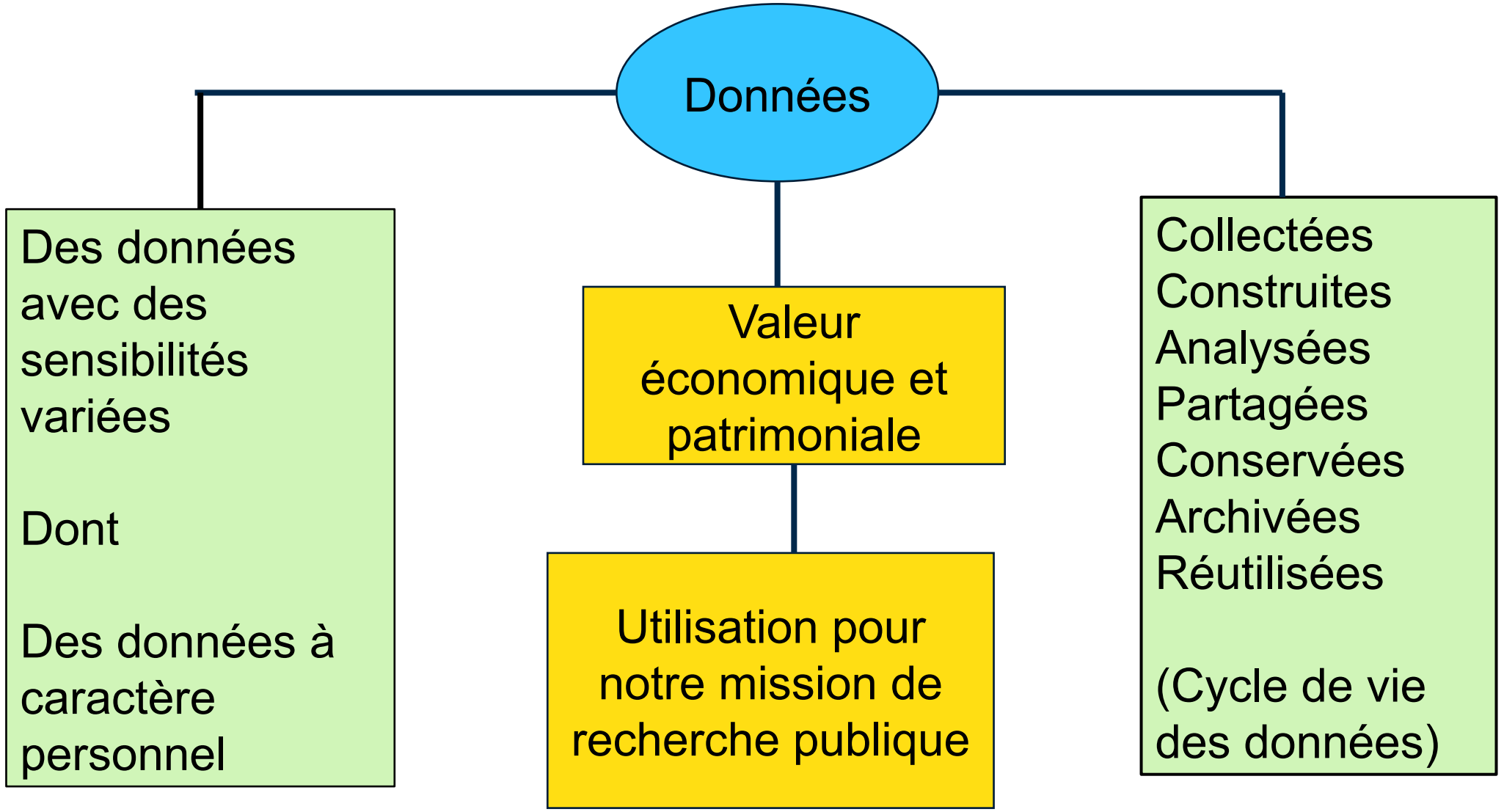
√ **Protection des données dans un environnement de risques numériques accrus : souveraineté numérique, PSSI**

√ **Ouverture de la science : Accès aux données, réutilisation à des fins de recherche scientifique (https://www.cnrs.fr/fr/donnees-ouvertes-de-la-recherche)**

√ **Protection du patrimoine scientifique et technique de l'Etat**

√ **Responsabilité sociétale et exemplarité (dont le respect des règlementations en vigueur)**

Quelles données dans les établissements de l'ESR ?



Le cycle de vie des données

« Le cycle de vie des données de la recherche est l'ensemble des étapes de gestion, conservation, diffusion et réutilisation des données scientifiques, associées aux activités de recherche. »

Deboin Marie-Claude. 2018. Découvrir de nouveaux métiers liés aux données de la recherche. Montpellier (FRA) : CIRAD, 5 p.

Documentation :
https://opidor.fr/ : dont PGD CNRS : https://opidor.fr/le-cnrs-publie-un-modele-de-pgd-structure-dans-dmp-opidor/

https://doranum.fr/ : apprentissage numérique de la gestion des données de la recherche

D'après Research data lifecycle – UK Data Service
https://www.ukdataservice.ac.uk/manage-data/lifecycle

La recherche et la protection des données : une compatibilité effective

Article 89 du RGPD : consacre l'utilisation des données personnelles à des fins de recherche et des dérogations possibles aux principes pour ne pas entraver la recherche (https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre9#Article89)

Une exception à l'ouverture des données: les données personnelles ne sont pas publiques et normalement non accessibles. Mais **réutilisation possible des données à des fins de recherche scientifique** : une articulation à trouver pour garantir la protection de la vie privée et permettre le progrès de la connaissance

Qu’est-ce que le RGPD ?

25 Mai 2018

Toute l’Union européenne

Tous les organismes traitant des données de personnes se trouvant dans l’UE

Périmètre

Applicable à :

- **Toute organisation** traitant des données à caractère personnel de **résident de l'UE**
- Toute organisation **hors UE** lorsque ses activités de traitement sont liées à une **offre de biens ou services** à l'égard de résidents de l’UE ou au **profilage** de celles-ci

Objectifs

- Renforcer la protection des **données à caractère personnel**
- Intégrer la **proactivité et la sécurité durant tout le cycle de vie** de la donnée

Ambitions

- Harmoniser le **droit de la protection des données personnelles** au sein de l’UE, en particulier avec la multiplication des échanges transfrontaliers
- **Renforcer les droits** des individus et **clarifier les obligations** des organisations

La protection des données personnelles : le cadre juridique

Règlement européen sur la protection des données RGPD

Directive Police Justice

Loi Informatique et Liberté modifiée

Cadre juridique commun : droit pénal, civil, administratif

Autres lois sectorielles : code du Patrimoine, code de la Santé publique, ….

Les risques en cas de non application du RGPD (non exhaustifs)

Risques financiers

Sanction CNIL

Perte de données

Risques juridiques

Responsabilité pénale

Action judicaire d'une personne

Risques médiatiques

Sanction publique de la CNIL

Fuite dévoilée par la presse

Risques Sur le patrimoine

Perte de données

Suppression données suite à sanction CNIL

Risques moraux

Perte de confiance en la recherche académique

Rupture confiance entre employeur et agent

02

Quelques définitions

Données à caractère personnel

Toute information se rapportant à une personne physique vivante (individu) identifiée ou identifiable (ci-après dénommée «personne concernée») .

Est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, 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.

Données à caractère personnel sensibles

Informations qui révèlent la prétendue 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.

Données personnelles de catégorie particulière

Principe d'interdiction de collecte mais des exceptions (article 9.2 RGPD)

- Le consentement : il doit être explicite, libre et éclairé
  (il ne s'agit pas du fondement légal du traitement mais le consentement est là nécessaire)

- Le traitement porte sur des données manifestement rendues publiques par la personne concernée

- Le traitement est nécessaire à des fins de recherche scientifique ou des fins historiques ou à des fins statistiques : (Avis de la CNIL nécessaire en cas de collecte de données sensibles auprès de personnes ne pouvant pas manifester leur consentement)

Les données anonymes

Il est impossible d'identifier par quelque moyen que ce soit une personne.

Trois critères du Comité européen de protection des personnes (CEPD) :

- Est-il possible d'isoler un individu ?
- Est-il possible de relier entre eux les enregistrements concernant un individu
- Est-il possible d'en déduire des informations le concernant ?

Les données pseudonymes

Restent des données personnelles : les données directement identifiantes sont remplacées par des données indirectement identifiantes.

La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires. En pratique la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, n, etc.). Il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces.

Anonymisation : Processus consistant à traiter des données à caractère personnel afin d'empêcher totalement et de manière irréversible l'identification d'une personne physique. L'anonymisation suppose donc qu'il n'y ait plus aucun lien possible entre l'information concernée et la personne à laquelle elle se rattache.

Pseudonymisation : est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires. En pratique la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) par des données indirectement identifiantes (alias, n, etc.). Il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces. C'est pourquoi des données pseudonymisées demeurent des données personnelles.
L'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Responsable de traitement

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Pour les structures rattachées au CNRS, le directeur d'unité, le délégué régional, le directeur d'un Institut, le directeur d'une direction fonctionnelle, etc… sont chacun responsables des traitements mis en œuvre dans les entités dont ils ont la responsabilité.

Traitement

Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés (format numérique ou papier).

Ex. : l'accès, la collecte, l'enregistrement, le stockage, le partage, l'utilisation, l'archivage ou l'effacement de données à caractère personnel.

Le sous-traitant

Prestataire, traite des données pour le compte du responsable de traitement, doit assurer une sécurité des données personnelles et aider le responsable de traitement dans la mise en œuvre de ses obligations

- Un contrat doit lier le RT et le(s) sous-traitant(s)

- Aider le RT dans la mise en œuvre de ses obligations (analyse d'impact sur la vie privée, notification de violation de données, sécurité)

- Tenir un registre des traitements effectués pour les RT

- Le RT est tenu de suivre le respect des obligations du sous-traitant

03

Les principes fondamentaux

Les principes à respecter

01 Définir une finalité/un objectif du traitement

02 Avoir un fondement légal (licéité)

03 Définir une durée de conservation

04 Minimiser les données collectées

05 Tenir à jour les données collectées

06 Sécuriser les données

07 Informer les personnes concernées

La finalité du traitement

- Les données doivent être collectées pour des finalités déterminées, explicites et légitimes

- Réutilisation pour d'autres finalités :
  En principe interdite ; sauf pour la réutilisation à des fins de recherche scientifiques -> Science ouverte

- Consécration de la recherche exploratoire :
  Le RGPD reconnaît qu'il peut être difficile de cerner entièrement la finalité

Les bases légales (article 6 du RGPD)

- Le consentement : la personne a consenti au traitement de ses données
- L'exécution d'un contrat : nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernées.
- L'obligation légale : traitement imposé par des textes légaux.
- L'intérêt légitime : le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées.
- L 'exécution d'une mission d'intérêt public.
- *La sauvegarde des intérêts vitaux (peu ou pas concerné au CNRS).*

Les bases légales (le plus souvent au CNRS)

- Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le RT :
  - La recherche publique est une des missions de service public
  - Cas particulier des recherches avec le privé, recherche avec certaines universités étrangères…

- Intérêt légitime du RT à moins que prévalent les intérêts de la personne concernée :
  - Lorsque la 1ère condition n'est pas possible
  - Attention quand il y a des mineurs

Exemples :
Dans le cas d'un projet mené dans une unité de recherche -> fondement mission service public.
Si ce projet est commandé par une entreprise privée -> intérêt légitime

Combien de temps conserver les données

Les données doivent être conservées pour la seule durée nécessaire à l'exercice de la finalité :

→ Appréciation de ces critères au regard de la finalité

→ A l'issue de cette période : archivage, anonymisation ou destruction (attention archives publiques)

→ Nouvel apport du RGPD : possible de conserver les données au-delà de cette période à condition de ne les traiter qu'à des fins de recherche scientifique

Minimiser les données collectées

Les données correspondent-elles à la finalité ? (principe de proportionnalité)

Les données doivent être pertinentes, proportionnelles et non excessives :

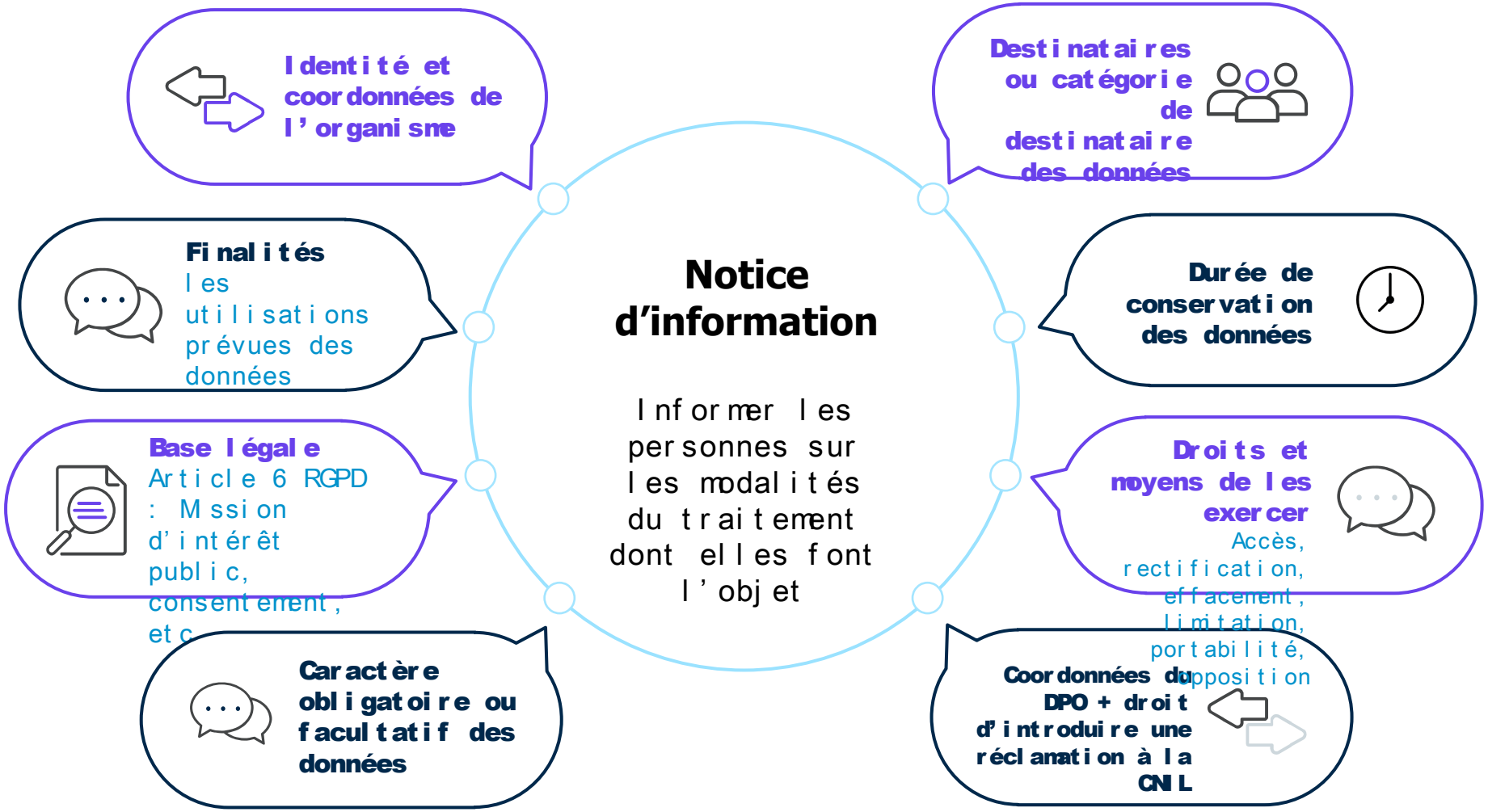
- Apprécier ces critères au regard de la finalité
- Se poser les bonnes questions :
  Ai-je besoin de ces données pour atteindre mes objectif de recherche?
  Puis-je minimiser ma collecte?

Exemple : pas nécessaire d'avoir des dates de naissance mais que des années la plupart du temps

Les droits des personnes (chapitre 3 RGPD : articles 12 à 23)

- Droit à l'information individuelle et transparente
- Droit d'accès
- Droit de rectification
- Droit à l'effacement
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit d'opposition

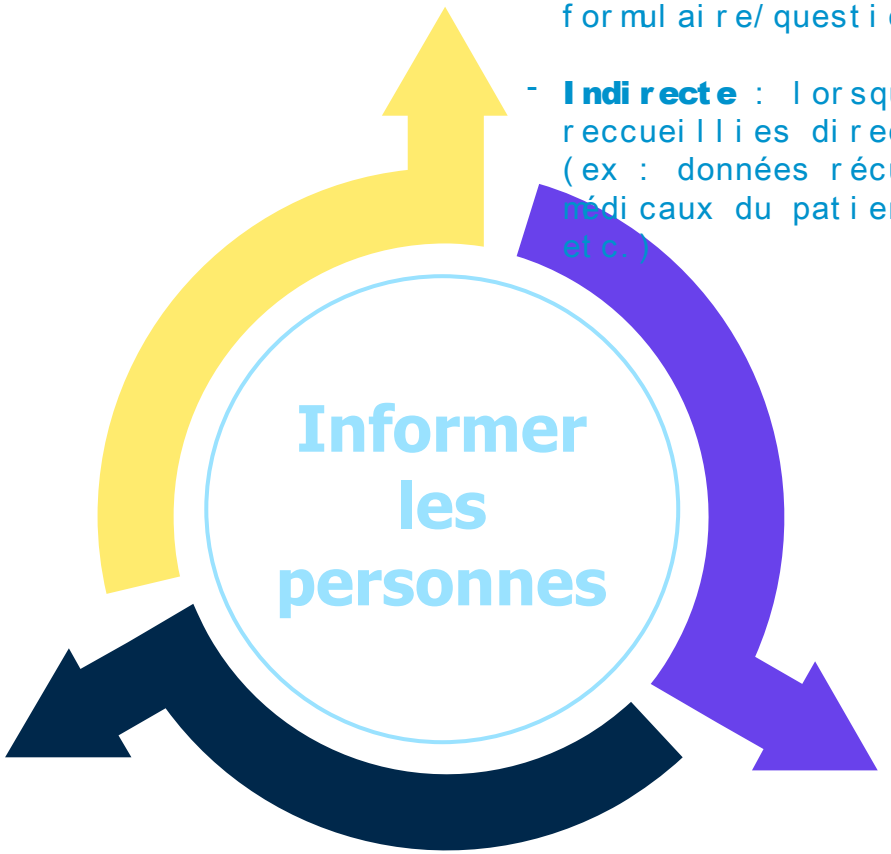
Notice d'information



Notice d'information

DÈS LA COLLECTE DES DONNÉES

- **Directe** : lorsque les données sont reccueillies auprès des personnes (ex : formulaire/questionnaire en ligne)
- **Indirecte** : lorsque les données ne sont pas reccueillies directement auprès des personnes (ex : données récupérées à partir des dossiers médicaux du patient, d'un partenaire académique, etc.)



SOUS QUELLE FORME ?

- Facile d'accès
- Fournie de manière claire et compréhensible
- Écrite de manière concise, afin d'amener les informations pertinentes

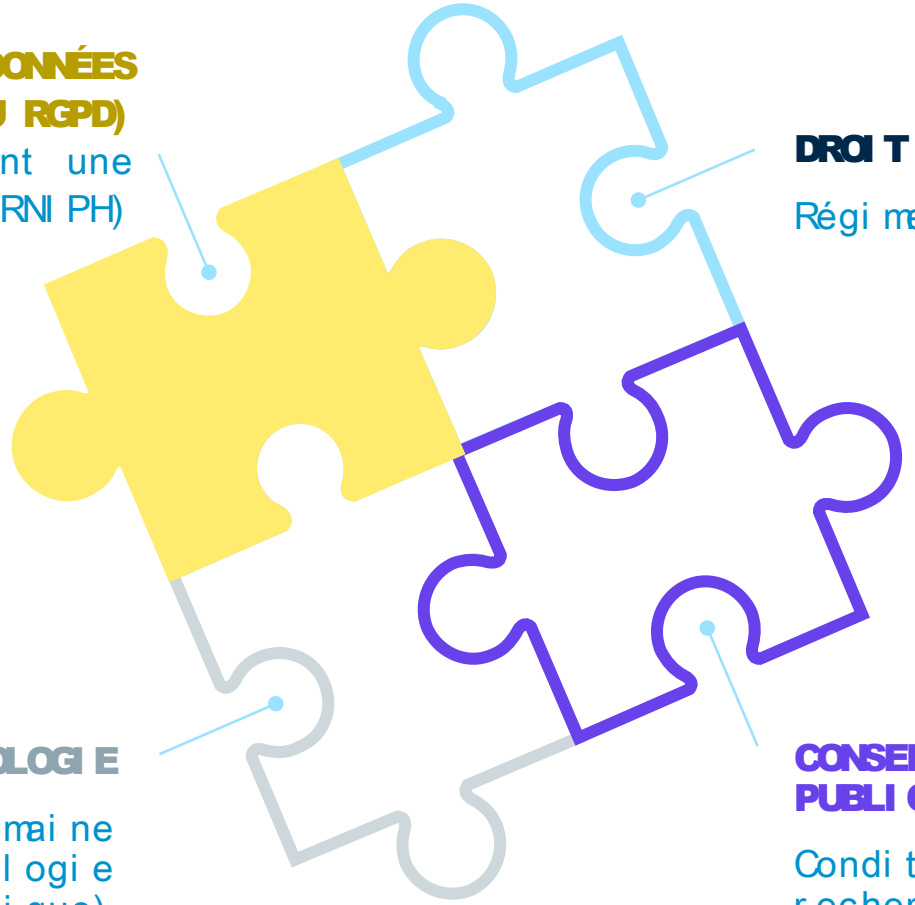
A QUEL MOMENT ?

- **Collecte directe** : au moment du reccueil des données
- **Collecte indirecte** : Dès que possible (notamment lors du premier contact avec la personne) et au plus tard, dans un délai d'un mois
- **Modification substancielle/ événement particulier** : nouvelle finalité, nouveaux destinataires, changement dans les modalités d'exercice de droits, violation de données

Consentements

CONSENTEMENT TRAITEMENT DONNÉES SENSIBLES (ARTICLE 9§2, A) DU RGPD)

Régime d'exception évitant une autorisation CNIL (hors RIPH et RNIPH)



DROIT A L'IMAGE ET À LA VOIX

Régime juridique distinct

CONSENTEMENT CODE DE DÉONTOLOGIE

Imposé dans certains domaine scientifique (ex : psychologie clinique)

CONSENTEMENT CODE DE LA SANTÉ PUBLIQUE

Condition de participation à la recherche clinique (RIPH 1 & 2)

Les dispositions pour assurer la sécurité et la confidentialité des données (article 32 du RGPD)

- Mesures techniques et organisationnelles : appui sur la PSSI de l'Etat mise en œuvre dans les établissements de recherche (La PSSI indique que les données personnelles sont des données sensibles)
- Dont : Changement régulier des mots de passe ; chiffrement des ordinateurs, téléphones portables et autres supports numériques ; réalisation régulière de sauvegardes des données …
- Toutes les unités ne disposent pas des ressources suffisantes et importance de s'appuyer sur les services offerts : Offre de service du CNRS, Renater, DataCenter, HumaNum pour les SHS, offre des tutelles partenaires

- Selon le niveau de risque et de sensibilité des données : une analyse d'impact sur la vie privée (AIPD) est obligatoire lorsque les risques sont élevés pour la personne concernée

- Pour déterminer le niveau de risque, Cf. CNIL :

  https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Les dispositions pour assurer la sécurité et la confidentialité des données

Le RGPD intègre une obligation de sécurité (art 32)

1. La sécurité doit être proportionnée aux risques
2. Les risques concernent
   - Les accès non autorisés (confidentialité)
   - Les modifications non désirées (intégrité)
   - La disparition de données (disponibilités)

3. La source de ces risques
   - Interne
   - Externe
   - Accidentelle
   - Délibérée

4. Exemple de parade
   - Chiffrement
   - Pseudonymisation

Les dispositions pour assurer la sécurité et la confidentialité des données

Bonnes pratiques

UTILISATEUR

1 / Choisir avec soin ses mots de passe

Ne jamais inscrire de mot de passe sur papier – Utilisation coffre fort KeePass – KeePassDroid – SyncPass

2/ Séparer les usages personnels des usages professionnels

Ne pas stocker des données professionnelles sur support personnel (USB,DD,cloud)

3/ Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Attention aux informations sur réseaux sociaux

4 / Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Pas d'enregistrement de mot de passe

Les dispositions pour assurer la sécurité et la confidentialité des données

Bonnes pratiques

LES RELATIONS EXTERIEURES

5 / Être prudent lors de l'utilisation de sa messagerie
Demande de login/pwd = mail frauduleux

6 / Naviguer avec un compte utilisateur
Ne jamais surfer avec un compte admin

7 / Être vigilant lors d'un paiement sur Internet : https://

8 / Protéger ses données lors de ses déplacements
Surveiller son matériel – En voyage juste le nécessaire (données)

Les dispositions pour assurer la sécurité et la confidentialité des données

Bonnes pratiques

DANS L'ESPACE PERSONNEL OU AU CNRS

9 / Effectuer des sauvegardes régulières
Ransomware - Attention au Cloud

10 / Mettre à jour régulièrement vos logiciels y compris les antivirus

11 / Télécharger ses programmes sur les sites officiels des éditeurs

12 / Sécuriser l'accès Wi-Fi de votre entreprise

Les dispositions pour assurer la sécurité et la confidentialité des données

LES 9 BONNES PRATIQUES EN UN COUP D'ŒIL

AVANT	**1** Évitez le transport de données superflues	**2** Informez-vous sur la législation du pays de destination	**3** Sauvegardez les données que vous emportez	
PENDANT	**4** Faites preuve de discrétion	**5** Évitez de laisser vos documents et équipements sans surveillance	**6** Évitez de vous connecter aux réseaux ou équipements non maîtrisés	**7** Informez votre responsable de la sécurité en cas de perte ou de vol
APRÈS	**8** Renouvelez les mots de passe utilisés lors de votre déplacement	**9** En cas de doute, faites vérifier vos équipements par votre responsable de la sécurité		

04

Au CNRS, les pratiques

Les acteurs et leur rôle

► Le chercheur, l'ingénieur, le technicien, le doctorant dans sa structure = chargé de la mise en œuvre

► Le directeur d'unité = responsable de traitement (dans les unités CNRS)

► Les prestataires extérieurs, sous-traitants

► Les responsables des établissements

► Les délégués à la protection des données

► La Commission Nationale Informatique et Libertés (CNIL)

Les acteurs et leur rôle

► **Le responsable de traitement** : Est la personne, l'autorité publique, le service ou l'organisme qui détermine la finalité et les moyens des traitements mis en œuvre -> Pour les unités CNRS = DU

Les obligations des RT :

- Tenir un registre des traitements et y inscrire les traitements
- Organiser et assurer la sécurité des données personnelles collectées
- Faire droit aux demandes de modification des données personnelles par les personnes concernées

- Les registres sont tenus par la DPD du CNRS (pour les unités accompagnées par le CNRS) : registre des traitements, registres des sous-traitants, registres des demandes d'accès aux données, registre des violations de données

Les accords contractuels au CNRS

- Les prestations de services avec clauses dédiées à la protection des données
- Les accords de collaboration avec clauses dédiées à la protection des données
- Les contacts au CNRS : les services partenariat et valorisation des délégations régionales
- Modèles sur l'intranet du CNRS : https://intranet.cnrs.fr/Cnrs_pratique/juridique/modeles/Pages/contrats.aspx

L’accompagnement du CNRS : le service protection des données

Actions centrées sur un objectif général : Contribuer aux missions du CNRS pour le progrès de la connaissance et du développement économique, social et culturel de la société

La protection des données personnelles s’inscrit dans une démarche éthique :

- Apporte la sécurisation de ses activités, une sécurisation des données traitées et fiabilité des recherches
- Contribue à la confiance de la société dans la recherche, dans le numérique
- Contribue à la gestion quotidienne sereine du CNRS

- Documentation, modèles de documents : site intranet dédié :

https://intranet.cnrs.fr/protection_donnees/rgpd/Pages/default.aspx

Un traitement de données personnelles ? Les questions à se poser

- Quelles natures de données ?
- Pourquoi suis-je autorisé à traiter des données ? (fondement légal)
- Quelle est la finalité ?
- Quels sont les acteurs ? Leur rôle ? Leurs responsabilités ?
- Les données correspondent-elles à la finalité ? (proportionnalité)
- Combien de temps conserver les données ?
- Les personnes sont-elles informées ?
- Les données et le traitement sont-ils bien sécurisés ?

Les actions pour une validation de la conformité RGPD

- Contacter le délégué à la protection des données désigné de l'unité.
- Transmettre tous documents se rapportant au traitement : synthèse du projet de recherche ; notes d'information, éléments sur les mesures de sécurité des données

Le DPO à l'honneur

Les outils et applications au CNRS

- Initier les formalités sur Revcil : https://revcil.cnrs.fr

Ou : Formulaire à compléter : https://intranet.cnrs.fr/protection_donnees/rgpd/application/Pages/declarer_fichier.aspx

Le Service Protection des Données : dpd.demandes@cnrs.fr
Téléphone : 08.83.85.64.26

Les violations de données personnelles

Définition : Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

Réflexe : informer en cas de suspicion : Directeur unité, DPD, responsable sécurité des Systèmes d'Information de l'unité

Prendront des mesures immédiates sont pour remédier à l'incident de sécurité source de la violation et minimiser les conséquences sur la vie privée des personnes,

Liens utiles

- Guide Recherche SHS et RGPD : https://www.inshs.cnrs.fr/sites/institut_inshs/files/pdf/Guide_rgpd_2021.pdf
- Intranet CNRS : https://intranet.cnrs.fr/protection_donnees/rgpd/Pages/default.aspx
- Sécurité : https://securite-si.cnrs.fr/
- Guide CNIL : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

- **Des appuis dans les unités :**
- https://www.huma-num.fr/
- https://www.progedo.fr/
- https://mate-shs.cnrs.fr/ et https://mate-shs.cnrs.fr/les-groupes/so-mate-mate-shs-sud-ouest-2/

05

Focus Science ouverte

Ce qu’est la science ouverte

- Depuis la Loi pour une république numérique de 2006, la science ouverte permet de « rendre accessible, autant que possible, et fermé autant que nécessaire » les résultats de la recherche issus notamment de fonds publics.
- En pratique : les données produites par un établissement administratif (de recherche) sont des données publiques
- Par extension, les données produites en vue de la publication, sont des données publiques et donc soumises au principe d’ouverture par défaut et de réutilisation gratuite, sauf si elles relèvent d’une des exceptions fixées par la loi.
- Les exceptions au principe d’ouverture par défaut : Certaines données non communicables ; exemples : secret défense, sécurité intérieure ; Des règlementations spécifiques : RGPD, droit de la propriété intellectuelle ;

Ainsi, les données personnelles ne sont pas accessibles en open data

Ce que prévoit le RGPD

- Les données personnelles sont « collectées pour des finalités explicites, légitimes et déterminées et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités » (article 5).
- Les traitements ultérieurs à des fins archivistiques, de recherche scientifique ou historique, à des fins statistiques ne sont pas considérés incompatibles avec la finalité initiale (article 89 du RGPD)

Une réutilisation possible des données à des fins de recherche scientifique : une articulation à trouver pour garantir la protection de la vie privée et permettre le progrès de la connaissance

Anticiper la réutilisation possible

Assurer la conformité à la règlementation sur la protection des données et prévoir la réutilisation des données le plus en amont possible : quelles données, qui pourra les utiliser, comment y accéder ?

Avoir informé les personnes participant à la recherche de la réutilisation possible de leurs données pour d'autres projets à finalité scientifique

Protéger les données : pseudonymisation, hébergements dans des entrepôts sécurisés, licences

Le partage des données personnelles

- Situation 1 : Les données personnelles sont collectées, traitées et anonymisées (aucune réidentification possible) :

Les données peuvent être accessibles en open data

- Situation 2 : Les données, jeux de données sont pseudonymisés

- Situation 3 : Les données sensibles et indirectement identifiantes sont accessibles dans des entrepôts sécurisés (CASD, entrepôts de données de santé)

Les données peuvent être réutilisées avec des modalités techniques et organisationnelles qui permettent de protéger les personnes

Les précautions

- Avant toute réutilisation des données : vérifier les conditions d'accès aux données et la conformité à la règlementation en matière de protection des donnés personnelles

- Respecter les principes du RGPD, contacter la DPD et valider la conformité au RGPD (en tenant compte des spécificités telle les difficultés d'information individuelle des personnes)

06

Questions ?