Déléguée à la protection des données

INRA SCIENCE & IMPACT

Règlement Général sur la Protection des Données - RGPD -

Nathalie Gandon - *Inra*

RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

(ou GDPR pour: General Data Protection Regulation)

Texte de référence européen en matière de protection des données personnelles pour les résidents de l'U.E

25 MAI 2018

POUR QUI?

(publics / privés) européens mais aussi les établissements basés hors UE qui collectent, et/ou hébergent, et/ou manipulent des données personnelles de citoyens européens.

Définitions

- **Quand ?**
  Lorsqu'on utilise des **données à caractère personnel (DCP)** / Sphère privée, professionnelle ou publique

Tous les aspects de la vie d'un individu identifié directement (nom, prénom) ou indirectement (voix, NIR, n° tel) par recoupement d'informations
Éléments physiques, psychologiques, génétiques, mentaux, économiques, culturels, sociaux, techniques (données de connexion, géolocalisation)…

DCP interdites de collecte / DCP dites *Sensibles ou Particulières*
Information concernant l'origine raciale ou ethnique, les opinions politiques, convictions philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle, données génétiques et données biométriques (aux fins d'identification).

Exceptions à la collecte de DCP sensibles :
- Consentement explicite des personnes ;
- Données rendues publiques par la personne concernée;
- Nécessaire aux fins de recherche scientifique;
- …

Définitions

DCP de santé : Données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique qui révèlent **des informations sur l'état de santé de cette personne**.

Sont comprises : *les informations collectées lors de l'inscription (d'un individu) en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ; toute information concernant, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro.*

Données hautement personnelles : relatives aux communications électroniques, à la géolocalisation et aux données financières

Définitions

- **Traitement de DCP :**

  Toute opération portant sur des DCP ayant un fondement juridique (licéité)

  Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...

- **Responsable de traitement (RT) ?**
  - L'autorité publique, service ou organisme qui détermine la finalité des traitements de DCP et les moyens nécessaires à leur mise en œuvre, notamment informatiques.
  - Doit démontrer la conformité de ses traitements de DCP au RGPD

Pour les unités de recherche INRA (mixtes ou propres), le **Directeur d'unité est le RT** *(doctrine CNIL reprise par CNRS, CPU et INRA)*

- Le RT fait la démarche de désignation du Délégué à la Protection des Données (DPD) de son unité
- Le DPD pressenti est mis en mesure d'accepter ou de refuser cette désignation

Principes de protection des données / Démarche éthique à démontrer

❑ Principe 1 – Finalité du traitement limitée

Les DCP sont collectées pour un usage déterminé, explicite et légitime.

Elles sont traitées de manière licite, loyale et transparente par rapport à la personne concernée.

Elles ne sont pas traitées ultérieurement d'une manière incompatible avec la finalité initialement définie.

Exception au traitement ultérieur : à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (art. 89 §1)

❑ Principe 2 - Proportionnalité et pertinence de la collecte

Seules les informations pertinentes et nécessaires au regard des objectifs poursuivis doivent être traités (minimisation des données)

❑ Principe 3 - Durée de conservation / Délai d'effacement

Pas de conservation des DCP indéfinie dans les fichiers informatiques. Une durée doit être définie obligatoirement en fonction de l'objet de la recherche.

Au-delà : archivage, effacement, anonymisation (sauf traitements ultérieurs art. 89 si mesures organisationnelles et techniques sont prévues pour garantir les droits des personnes).

❑ Principe 4 - Sécurité, intégrité, confidentialité

Les DCP sont sécurisées au regard de leur sensibilité et des risques évalués sur la vie privée, y compris contre la perte, destruction ou l'utilisation ou la ré-utilisation non autorisée.

❑ Principe 5 - Droits des personnes renforcés

Les personnes dont les DCP sont collectées doivent être informées du traitement de leur données et les droits qui leurs sont conférés respectés : accès, rectification, suppression, opposition/consentement… (arts. 12 à 22)

Principaux changements – Plus de responsabilités

LE RGPD introduit un changement des pratiques mais pas des principes

Principe de responsabilisation ou « Accountability » / renversement de la charge de la preuve :

Le responsable de traitement doit pouvoir prouver à tout moment sa conformité au RGPD, ce qui exige la mise en place d'une traçabilité via un système documentaire. A l'INRA, on parle de **dossier de conformité qui regroupe divers formulaires**.

Les formalités auprès de la CNIL sont presque toutes supprimées, elles se font désormais en interne des établissements.

Une personne mécontente n'a pas besoin d'apporter de preuve de la non-conformité : c'est au responsable de traitement mis en cause de démontrer sa conformité.

Etude d'impact sur la vie privée (EIVP ou PIA « Privacy Impact Assessment ») :

Pour tout traitement porteur de risques élevés pour les personnes concernées, il devra obligatoirement réaliser une EIVP afin d'adapter les mesures de sécurité.

Privacy by design/ by default :

Tout traitement et/ système d'information doit être pensé dès le début pour respecter la vie privée et donc respecter les 5 grands principes.

Principaux changements – Nouveau statut pour le sous-traitant

- Organisme (développeur informatique), service (autre équipe de recherche, plate-forme), personne physique (transcripteur par ex.) qui agit pour le compte de l'unité sans être du même organisme ou UMR.

La qualification RT et ST est importante pour la rédaction des contrats / marchés qui doivent contenir une description de la prestation ainsi que les obligations de sécurité et les clauses spécifiques obligatoires de protection des DCP (art. 28).

- Aide le RT à garantir le respect de ses diverses obligations et doit l'alerter si celui-ci paraît commettre un manquement ;
- Ne sous-traite pas sans autorisation écrite et sans rappel des obligations du ST ;
- Est tenu responsable en cas de non-respect de ses obligations propres ou des instructions licites du RT (saisine CNIL + recours juridictionnel).

Certaines clients privés de plates-formes publiques demandent désormais à celles-ci la preuve de leur conformité au RGPD et prévoient de venir mener des audits.

Principaux changements – Sécurité

- Article 32 : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

  a) la pseudonymisation et le chiffrement des données à caractère personnel;
  b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
  c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
  d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

- Autre nouveauté : Obligation de notification de violation des données personnelles à la CNIL et auprès des personnes concernées.

Principaux changements – Sécurité

Les différents types de sécurité

- Sécurité physique : par exemple hébergement dans un data center,
- Sécurité logique : par exemple chiffrement ou a minima pseudonymisation quand c'est nécessaire (données sensibles, confidentielles, etc.),
- Sécurité organisationnelle : par exemple une gestion des habilitations à accéder aux DCP collectées à mettre en place.

Principaux changements – Privacy by design

- Article 25 : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »

Principaux changements – Privacy by design

Le SI doit avoir les fonctionnalités techniques minimales requises en matière de sécurité à toutes les étapes et par exemple :

-Intégration des problématiques RGPD dès le début du projet,
-Gestion des droits d'accès (quelle politique de mot de passe?),
-Possibilité de requête sur le nom d'une personne afin de répondre aux demandes d'accès,
-Possibilité d'effacer les données concernant une personne en cas d'exercice du droit d'opposition,
-intégration des durées de conservation, purge automatique vers un archivage pérenne ou une destruction,
-intégration d'une technique d'anonymisation,
-quel hébergement pour les données (contrat avec ST, transfert hors UE?)
-etc.

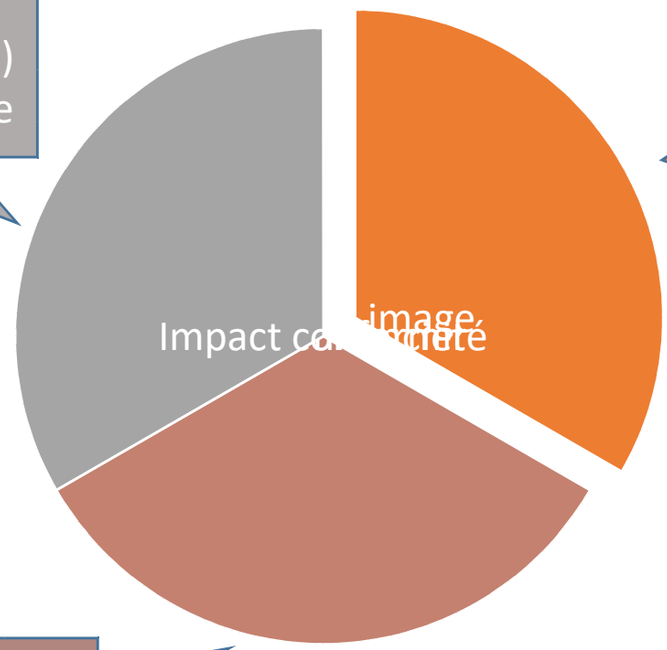
Existence de check list pour aider à balayer tous les points à prendre en compte.

Les risques pour l'ESR

Exemples d'infractions

- Traitement malgré l'opposition de la personne
- Détournement de finalité
- Absence d'analyse d'impact
- Absence de coopération avec l'autorité de contrôle
- Etc.

La non-conformité est un motif de non attribution de subventions de recherche



Nouveauté :
Action en justice possible via des actions de groupe

CONTRÔLES

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

-sur programmation annuelle,
-sur instruction d'une plainte,
-sur connaissance d'une violation de DCP (via presse ou directement par l'entreprise concernée).

A l'INRA

- Un **site intranet informatif** et où tous les documents de référence sont accessibles : https://intranet.inra.fr/cil-dpo
- Des sensibilisations et formation possibles à la carte,
- La mise en place du **dossier de conformité** et des différentes procédures, une Note de Service 2019-28 : https://intranet.inra.fr/cil-dpo/Mettre-en-conformite-mon-traitement/Remplir-le-dossier-de-conformite
- L'utilisation d'**Ariane** pour notifier un incident sur des données personnelles: https://ariane.inra.fr/block/create_security_incident.do?srv=cil
- Une adresse générique pour toutes vos questions : cil-dpo@inra.fr

Déléguée Informatique et Liberté (DIL) INRA: Nathalie Gandon
Juriste Informatique et Libertés INRA : Clémence Pascal

Merci de votre attention.
Des questions?