LA PROTECTION DES DONNÉES ET LES CNR

LE RGPD APPLIQUÉ AUX MISSIONS DES CNR

Séminaire CNR 15/11/2019

Clothilde Hachin, DPO, Santé publique France

RGPD : LES DATES

1974: SCANDALE SAFARI →**1978: LOI « INFORMATIQUE ET LIBERTÉS » (LIL) : LOI N°78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS**

- Création de la CNIL (Autorité administrative Indépendante)
- Encadrement des fichiers de « données nominatives »

2004: TRANSPOSITION DE LA DIRECTIVE 95/46/CE PAR LA LOI N°2004-801 DU 6 AOUT 2004

- Introduction de la notion de « données à caractère personnel »
- Renforcement des droits des personnes
- Modification/ durcissement des formalités

2016: RÈGLEMENT EUROPÉEN GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD) *– entrée en vigueur le 25 mai 2018:*

→Loi du 20 juin 2018 relative à la protection des données personnelles ;

→Ordonnance du 12 décembre 2018 [..] relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

LE RGPD – LES OBJECTIFS

Objectifs: simplification des procédures- renforcement des droits des personnes - responsabilisation des acteurs

→ **Renforcement de la sécurité juridique des échanges en UE:** pose un cadre commun

→ **Renforcement de la maitrise des personnes sur leurs données**: information renforcée +création de nouveaux droits et encadrement plus strict de certaines pratiques dont le profilage

→ **Renforcement de la responsabilité de tous les acteurs du traitement de données**: responsable de traitement mais aussi sous-traitant :

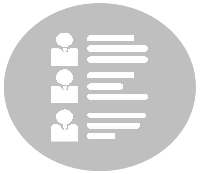
- **Accountability** (art. 5 et 24 RGPD): Passage d'un contrôle a priori à un contrôle a posterior*i* :
- ***Augmentation du montant des amendes administratives (****article 83 RGPD)*

TERRITORIALITÉ:

-Responsable de traitement sur le territoire UE

-Responsable de traitement hors UE mais qui traite des données relatives à des personnes résidant en UE

RGPD : LES NOTIONS CLÉS – ART. 4 RGPD



Données à caractère personnel

Toute information relative à une personne physique **identifiée ou pouvant être identifiée**

Quid des données de santé?

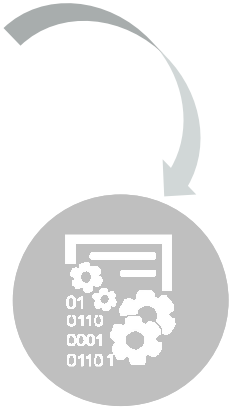
pseudonymisation

Responsable de traitement (RT)

Personne physique ou morale qui détermine la **finalité** et les **moyens du traitement**

Nouveautés RGPD:

- Responsable conjoint (article 26 RGPD)
- Responsabilisation du sous-traitant (STT) (art.28 RGPD)
- CIL→DPO (data protection officer- art.37 RGPD)



Traitement de données

Toute manipulation **automatisée ou non** de données

RGPD: LES OBLIGATIONS

DATA PROTECTION BY DESIGN AND BY DEFAULT (art. 25 RGPD)

OBLIGATIONS DE « FOND » - art. 5 RGPD : impactent la structure même du traitement

1. Licéité du traitement: Une base légale identifiée au regard de l'article 6 RGPD

2. Limitation des finalités: Une finalité légitime et déterminée

3. Minimisation des données: Adéquation des données collectées à la finalité

4. Limitation des données: Adéquation de la durée de conservation à la réalisation de la finalité;

5. Loyauté et Transparence: Information préalable complète et respect des droits des personnes (retrait consentement, opposition, rectification, effacement, limitation, portabilité)

-Le consentement exprès n'est pas toujours requis

-Dérogations à l'obligation d'information individuelle strictement énumérées (et interprétées)

-Les droits des personnes sont définis en fonction de la base légale du traitement

NB: Information sur les *violation des données (art. 33 et 34 RGPD)*

6.Intégrité et confidentialité: garantir une sécurité appropriée des données à caractère personnel (cf. article 32 RGPD)

RGPD : LES OBLIGATIONS

OBLIGATIONS DE « FORME »: Impactent le calendrier

« Formalités préalables »

→ Objectif : vérifier et documenter la conformité du traitement à la loi avant sa mise en œuvre.

→**RGPD: Principe d'Accountability** (art. 5 et 24 RGPD) **:** *Vers un contrôle a posteriori - fin des déclarations préalables :*

-**Registre de tous les traitements (**art. 30 RGPD) ≠ Registre CIL : seulement les déclarations

-Introduction d'une **Analyse d'impact sur la protection des données** (***AIPD ou PIA –*** *art. 35 RGPD*): traitement présentant un risque élevé pour les droits et libertés des personnes

→Possibilité d'une AIPD pour des traitements similaires

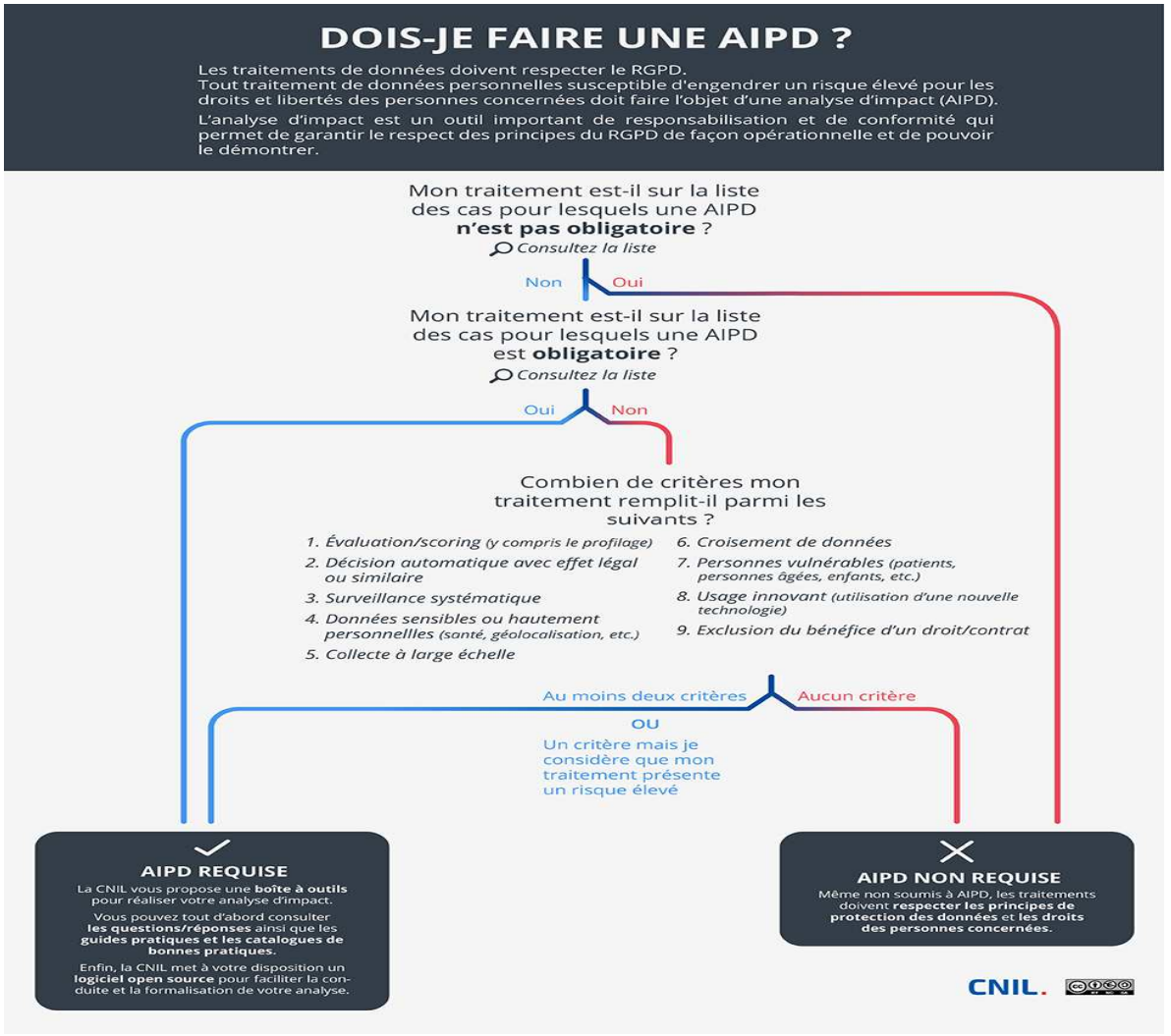
→Réévaluation

- **Consultation de la CNIL** lorsqu'à l'issue du PIA, risques non minimisés (art.36 RGPD);

- En France: **Autorisation CNIL** pour les traitement de données de santé (sous réserve d'exception strictement énuméré par article 65 LIL).

RGPD : LES OBLIGATIONS – AIPD/PIA

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



RGPD : LES OBLIGATIONS – AUTORISATION SANTÉ

- **Autorisation CNIL** pour les traitements de données à caractère personnel de santé (art. 64 et suivants LIL):

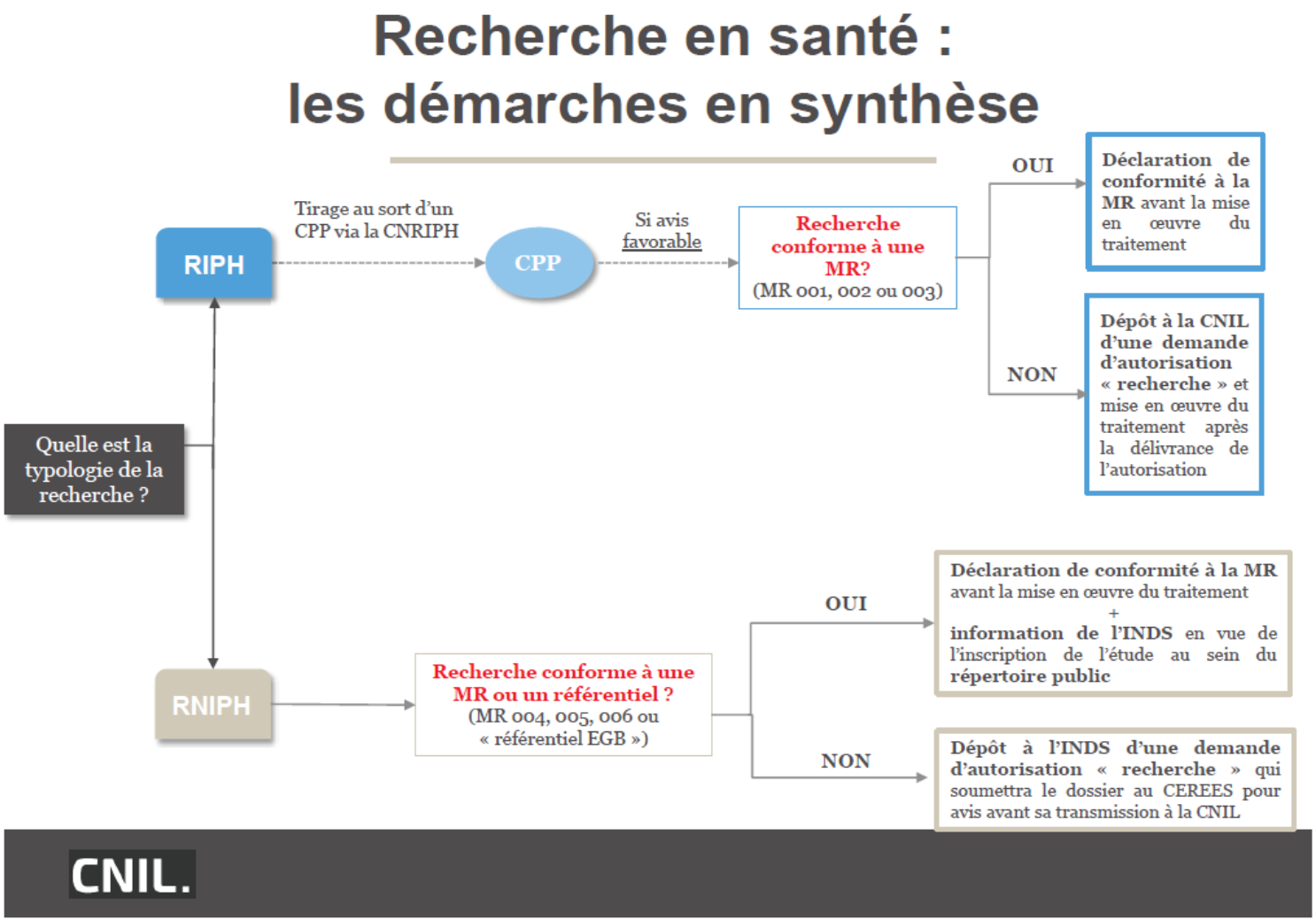
- Traitements de données à caractère personnel de santé ayant une finalité d'intérêt public
- Traitement de données à caractère personnel de santé mis en œuvre dans le cadre d'une « Recherche, étude, évaluation dans le domaine de la santé »

- **Exceptions à l'obligation d'autorisation** (art. 65 LIL):

•Les traitements pour lesquels la personne concernée a donné son **consentement exprès** (sauf si recherche impliquant la personne humaine ou données couvertes par le secret médical) ;
•Les traitements nécessaires à la **sauvegarde de la vie humaine** ;
•Les traitements portant sur des **données à caractère personnel rendues publiques par la personne concernée** ;
•Les traitements nécessaires aux fins de la **médecine préventive**, des **diagnostics médicaux**, de **l'administration de soins ou de traitements**, ou de la **gestion de services de santé** et mis en œuvre par un **membre d'une profession de santé** ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de **secret professionnel** (ex : dossier médical ou logiciel de gestion médico-administratif, télémédecine, PACS utilisé dans le domaine de l'imagerie médicale, etc.) ;
•Les traitements permettant d'effectuer des **recherches à partir des données réalisées par le personnel assurant ce suivi, et destinées à leur usage exclusif (recherche « interne »)** ;
•Les traitements mis en œuvre aux fins d'assurer le **service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie** ainsi que la **prise en charge des prestations par les organismes d'assurance maladie complémentaire** ;
•Les traitements effectués au sein des établissements de santé par les **médecins responsables de l'information médicale,** dans le cadre du pmsi local ;
•Les traitements effectués par les **agences régionales de santé**, par l'Etat et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du code de la santé publique et dans le cadre défini au même article ;
•Les traitements de données dans le domaine de la santé mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la CNIL, ayant pour seule finalité de répondre, en cas de situation d'urgence, à une **alerte sanitaire** et d'en gérer les suites.

RGPD : LES OBLIGATIONS – AUTORISATION RECHERCHE EN SANTÉ (LOI 2016- MODERNISATION SYSTÈME DE SANTÉ)

Santé publique France



Source: CNIL, *Atelier RGPD : la recherche dans le domaine de la santé*, 18 juin 2019, Service santé

CONSULTER VOTRE DPO

Documentation minimale pour chaque traitement:

1/ Protocole justifiant de la prise en compte des obligations de « fond »: finalités, fondement légale, responsable de traitement/sous-traitant, liste des données, durée de conservation, **modalités d'information et d'exercice des droits**, identification de la localisation des données et des mesures de sécurité

2/ Documents contractuels pour les relations avec les personnes intervenants dans le traitement (responsables conjoints, sous-traitants, destinataires des données)

3/ « formalités » préalables:

- **Inscription au registre du responsable de traitement**
- **AIPD/PIA** quand risque élevé pour les droits et libertés des personnes voire **autorisation (données de santé)**

RGPD APPLIQUÉ AUX MISSIONS DES CNR

- Quels traitements sont mis en œuvre dans le cadre des missions d'un CNR?

- Expertise
- Conseil
- Contribution à la surveillance épidémiologique
- Alerte

- Quel est le fondement légal des traitements mis en œuvre pour la réalisation des missions de CNR?

→Exécution d'une mission d'intérêt public: art. L. 1413-3, R. 1413-46 et suivants du code de la santé publique (CSP)

→Prérogatives relatives aux transmissions de données et d'échantillons:

- art. L. 1413-8 CSP prérogative propre aux CNR
- art. L. 1413-6 et R. 1413-40 et suivants CSP –membre RNSP

- Responsabilité du traitement?

Une responsabilité conjointe CNR-Spfrance?

RGPD APPLIQUÉ AUX MISSIONS DES CNR

- Quelles catégories de données sont nécessaire pour réaliser chacun de ces traitements?

- Données directement identifiantes
- Données sociodémographiques
- Données cliniques
- Données biologiques
- Autres

+ *Coordination avec Santé publique France sur les données à lui transmettre*

- Combien de temps ces données doivent être conservées pour réaliser chacun de ces traitements?

+ *Coordination avec Santé publique France sur les données à lui transmettre*

- Comment informer les personnes et vers qui peuvent-elles exercer leurs droits?

*Proposition d'une **information mutualisée** avec renvoi sur le site de Santé publique France pour l'identification des CNR responsables de la gestion des droits des personnes (opposition, accès, rectification, effacement, limitation).*

RGPD APPLIQUÉ AUX CNR

- Quelles mesures de sécurité peuvent être mises en oeuvre?

Mesures techniques:

ex: sécurisation des postes de travail, journalisation des accès et revue des droits d'accès, chiffrement des transferts numériques (ex: bluefiles, GPG, Zed! MSsanté), etc…

Mesures organisationnelles:

Ex: pseudonymisation, séparation des données nominatives des données d'études, contrat, charte informatique, sensibilisation, etc…

- Quelles relations contractuelles doivent-être établies?

Sous-traitant? Responsable conjoint?

- Quelles « formalités » doivent-être réalisées?

- Inscription au registre + PIA/AIPD

- Traitement de données de santé ayant une finalité d'intérêt public: Autorisation unique?