Le RGPD et vous
Quel impact sur votre travail ?

Ségolène Aymé
Segolene.ayme@icm-institute.org
Café de la NeuroInformatique
05/07/2018

RGPD
GDPR

Mise en conformité avec le Règlement Général sur la Protection des Données

Mis en œuvre le 25 Mai 2018

Adaptation française: Loi n°2018-493 du 20 juin 2018

Les données à caractère personnel

IDENTITE

Identifiants (Nom, Email, pseudo, Adresse IP etc.)
Biométrie (Age, Sexe, ADN, empruntes digitales etc.)
Idéologie (Intérêts, opinion etc.)

RELATIONS

Réseaux sociaux (groupes, intérêts, « j'aime », durée d'inactivité etc.)
Liens (amis, famille, collègues etc.)

CONTENUS

Médias (Photos, vidéos etc.)
Conversation (SMS, appels, discussions sur les réseaux sociaux, mails etc.)

SANTE

Soins
Traitements
Dossier médical etc.

FINANCES

Revenus
Transactions etc.

COMPORTEMENT

Navigation sur internet Habitudes de consommation etc.

CONTEXTE

Géolocalisation, Itinéraires etc.

Les grandes composantes du RGPD

Politique

- **Lutte cybercriminalité , compétition dans l'innovation et la recherche**

Economique

- **Sanction économique (amendes > 3M)**
  Sanction image > dons

Social

- **Droits des personnes Protection de la vie privée e-santé**

Technologique

- **Moderniser outils et pratiques Gouvernance des données Maitrise de la donnée**

Environnemental

- **Instaurer la confiance**

Légal

- **Règlement européen**

Comprendre le GDPR : les enjeux et les bénéfices

- **Homogénéiser** le droit de la protection des données dans l'Union européenne
- **Responsabiliser** tous les acteurs de la chaîne de traitement impliquant des données personnelles pour limiter les vols de données et fuite de données
- **Améliorer la confiance** des consommateurs dans l'économie numérique et dans les entreprises conformes
- Faire appliquer **les principes de concurrence** au secteur des services numériques pour favoriser l'innovation
- **Renforcer** le niveau global de protection des entreprises contre la cybercriminalité

La France avait déjà un droit exigeant

La collecte et le traitement des données relatives à la santé n'étaient possibles depuis 2003 qu'aux conditions suivantes :

Avec le consentement éclairé de la personne

- Information individuelle
- Droit d'opposition et de retrait
- Droit d'accès et de rectification

Après autorisation de la CNIL

- Avis du CCTIRS sur la pertinence scientifique de la collecte de données
- Mesures de sécurité physiques pour le control d'accès
- Séparation identité/données médicales
- Control de l'accès informatique
- Gestion des habilitations d'accès aux données
- Chiffrement des bases de données nominatives
- Charte de sécurité pour les personnels du registre

Les obligations de sécurité en pratique

Sensibilisation des utilisateurs

Authentifier les utilisateurs

Gérer les habilitations

Tracer les accès et gérer les incidents

Sécuriser les sites web

Sécuriser les postes de travail

Encadre les développements informatiques

Protéger le réseau informatique interne

Sécuriser l'informatique mobile

Sauvegarder et prévoir la continuité d'activité

Encadrer la maintenance et la destruction des données

Sécuriser les serveurs

Protéger les locaux

Archiver de manière sécurisée

Gérer la sous-traitance

Sécuriser les échanges avec d'autres organismes

Les grands changements

- Une logique inspirée du modèle anglo-saxon
  - Allègement des obligations réglementaires
  - Responsabilisation accrue des acteurs
  - Logique de mise en conformité dynamique et continue
- Guichet unique européen:
  - démarches auprès d'une seule autorité pour l'ensemble de l'UE
- Responsabilité accrue des acteurs
  - Obligation de documenter l'ensemble des mesures techniques et organisationnelles prises pour garantir la conformité au règlement (Art.24)
  - Obligation de prendre en compte la protection des données dès la conception du projet *Privacy by design*
  - Obligation de réaliser des analyses d'impact (Art. 35)
  - Notification obligatoire de failles de sécurité dans les 72h qui suivent la prise de connaissance, à l'autorité de tutelle mais aussi aux personnes concernées (Art.33 et 34)

Les grands changements (2)

- Droits existants renforcés
  - Information détaillée mais concise, transparente, facile d'accès et intelligible
  - Consentement renforcé mais modernisé
  - Flexibilité dans l'interprétation de la définition du consentement dans le cadre de la recherche scientifique

- De nouveaux droits
  - Droit à l'oubli numérique avec une exception en matière de recherche (Art.17 (3) (d)
  - Droit à la portabilité des données (Art.20)
  - Transparence sur les failles de confidentialité
  - Encadrement du profilage pour la prise de décision individuelle
  - de nouvelles voies de recours en justice sur le fondement du non-respect du règlement

Les grands changements (3)

- Désignation obligatoire d'un délégué à la protection des données avec exigence de compétence (DPO)
  - rattaché directement à la direction générale
  - Responsable sensibilisation, formation, audit
  - point de contact pour les autorités de tutelle et les tiers
- Promotion de codes de conduite par type d'activité (Art.40)
- Mécanismes de certification et de labellisation
- Augmentation très significative des sanctions
  - 20 millions d'Euros ou 4% du chiffre d'affaire mondial
- Institution du Comité européen de la protection des données pour qu'il n'y ait pas de pays qui pénalise par des particularités
  - arbitre des différents entre autorité de contrôle

Interdiction des traitements de données de santé sauf dérogations (Art 9)

- Consentement explicite de la personnes
- Finalités de sécurité et de protection sociale
- Sauvegarde des intérêts vitaux de la personne
- Gestion des services de soin en santé
- Motif d'intérêt public
- Recherche scientifique et statistique sous réserve de garanties appropriées et spécifiques définies par le droit de l'Union Européenne ou les législations nationales
- Les Etats-membres sont autorisés à introduire des conditions supplémentaires en ce qui concerne le traitement des données génétiques ou des données concernant la santé (art.9.4)

Les adaptations dans le droit français
Loi n°2018-493 du 20 juin 2018

- Révision de la Loi Informatique et Liberté du 6 janvier 1978 et de la loi de modernisation de notre système de santé du 26 janvier 2016
- Les données sensibles incluent les données biométriques et génétiques
- Art 21 encadre le recours aux algorithmes basé sur le *Deep Learning* pour la prise de décision au niveau individuel
- La loi abaisse de 16 à 15 ans l'âge du consentement
- Pour les données de recherche:

autorisation par la CNIL après avis d'un CPP « Comité de Protection des Personnes » ou du CEREES « Comité d'Expertise pour les recherches, les études et le évaluations dans le domaine de la Santé »

Principaux changements introduits par le RGPD

Amendes : En cas de non-conformité, des amendes administratives pouvant aller jusqu'à un plafond de **4% du chiffre d'affaire annuel global** ou **20 M€** (montant le plus élevé retenu).

Analyse d'impact relative à la protection des données : Obligation de réaliser des analyses formelle d'impact si le traitement représente un **risque élevé pour les personnes.**

DPO : Un DPO (Délégué à la protection des données) est **requis** pour les organismes publics et les Instituts qui effectuent un **suivi régulier et systématique à grande échelle des personnes**.

Droits des personnes concernées : Droits des personnes étendus pour inclure le **droit à la portabilité des données** et le **droit à l'oubli**.

Territorialité : Le GDPR concerne toutes les organisations établies en Europe et celles **établies hors d'Europe, mais traitant des données d'Européens**.

Données sensibles : Les données sensibles incluent dorénavant les données **biométriques** et les données **génétiques**.

Registre : Les organisations doivent tenir à jour un **registre documentant tous leurs traitements** de données personnelles.

Consentement : Le consentement préalable à la collecte des données doit être **libre, spécifique, éclairé et univoque**. L'opt-out ne peux plus être utilisé.

Notification des violations : Obligation de notifier les cas de violation de données personnelles à **l'autorité de contrôle** dans les 72h suivant l'incident, ainsi qu'aux **personnes concernées** en cas de risque élevés pour elles.

Sous-traitants : Les sous-traitants peuvent être **tenus pour responsables**. en cas de violation de données. Les responsables de traitement doivent s'assurer du respect du GDPR par les sous-traitants.

Sécurité : Obligation de sécuriser les données personnelles, et recommandations spécifiques sur le chiffrement, l'anonymisation et la pseudonymisation.

Protection des données dès la conception : Obligation d'intégrer la protection des données personnelles dès la conception et le développement de nouvelles solutions (« **Privacy by design** »)

Comment atteindre la conformité

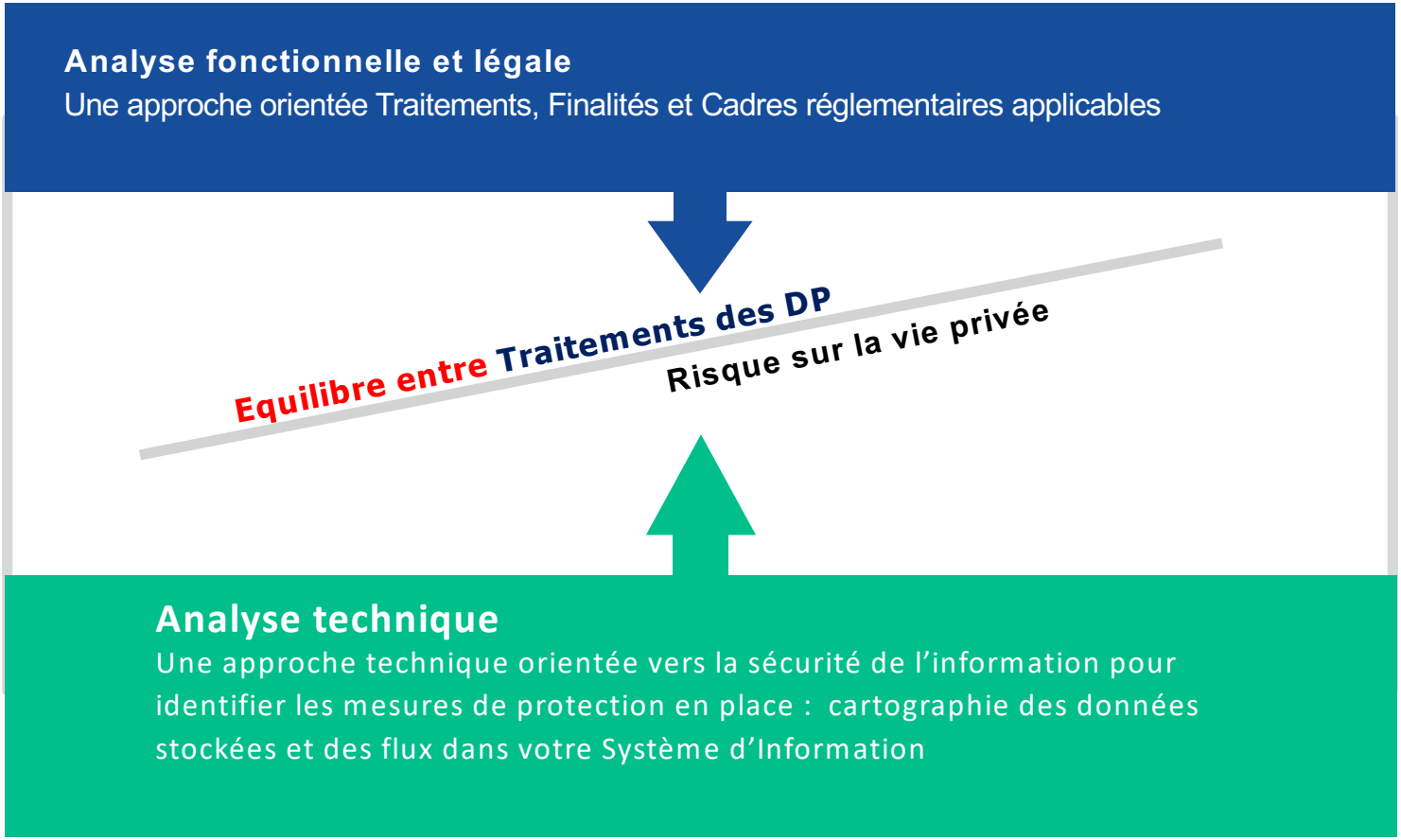
Méthode CNIL

Les recommandations de la CNIL pour…

- SENSIBILISER LES UTILISATEURS
- AUTHENTIFIER LES UTILISATEURS
- GÉRER LES HABILITATIONS
- TRACER LES ACCÈS ET GÉRER LES INCIDENTS
- SÉCURISER LES POSTES DE TRAVAIL
- SÉCURISER L'INFORMATIQUE MOBILE
- PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE
- SÉCURISER LES SERVEURS
- SÉCURISER LES SITES WEB
- SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ
- ARCHIVER DE MANIÈRE SÉCURISÉE
- ENCADRER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES
- GÉRER LA SOUS-TRAITANCE
- SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES
- PROTÉGER LES LOCAUX
- ENCADRER LES DÉVELOPPEMENTS INFORMATIQUES
- CHIFFRER, GARANTIR L'INTÉGRITÉ OU SIGNER
- ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES

Comment atteindre la conformité

Méthode CNIL



Le processus de mise en conformité à l'ICM

- DPO en cours de recrutement, en charge du pôle qualité
  - Dominique Bayle DSI

- Nomination de référents par secteur d'activité pour aider
  - Mécennat et communication
  - Ressources Humaines
  - Données cliniques

GÉRER LES HABILITATIONS

- Accompagnement du processus de mise en conformité par prestataire
  - Proposition 47 / Anyon

Périmètre des données et Méthodologie agile

Données ICM

Données des donateurs

Données RH

Données des patients et recherche:

- Santé
- Biométriques
- Génétiques
- Cliniques
- Démographiques

COM-DEV

DATA
SANTE
RECHERCHE
Equipes, Biobanques

RH

AUTRES

DF, DAR,
DAEL,DAMS
PLATEFORMES

...

Rapport de conformité

COM-DEV LOT1

SANTE RECHERCHE LOT2

RH LOT3

AUTRES LOT4

Démarche Globale

1

Audit, cartographie des traitements et des risques

Identification des enjeux autour des données à caractère personnel traitées par l'institut

2

Mise en conformité et Suivi

Définition du plan d'actions et établissement du socle documentaire
Suivi de la mise en oeuvre

3

Sensibilisation

Préparation des équipes à la mise en conformité au RGPD

Comment atteindre la conformité à votre niveau

Il est primordial de connaître :

- Les données manipulées et leur caractéristiques
- Les traitements réalisés sur ces données et leurs finalités
- Les composants du SI utilisés dans la manipulation de ces données
- vue orientée métier du parcours de la donnée et des finalités des traitements &
- vue technique de manipulation des données (stockage, transfert, suppression…) dans le système d'information.

Les étapes pour vous

- Identifier un référent dans chaque équipe concernée
  - Un guide méthodologique sera fourni après l'été
- Commencer la cartographie
  - Quelle données nominatives
  - Localisations (partenaires)
  - Supports de stockage (serveurs, cloud)
- Commencer la documentation de la gouvernance
  - Mesures de sécurité, physique et informatique
  - Qui a accès, comment, gestion des droits
  - Procédures et ressources pour faire valoir les droits

Bon courage

L'équipe NeuroInformatique vous accompagne