10/13 JuriSanté

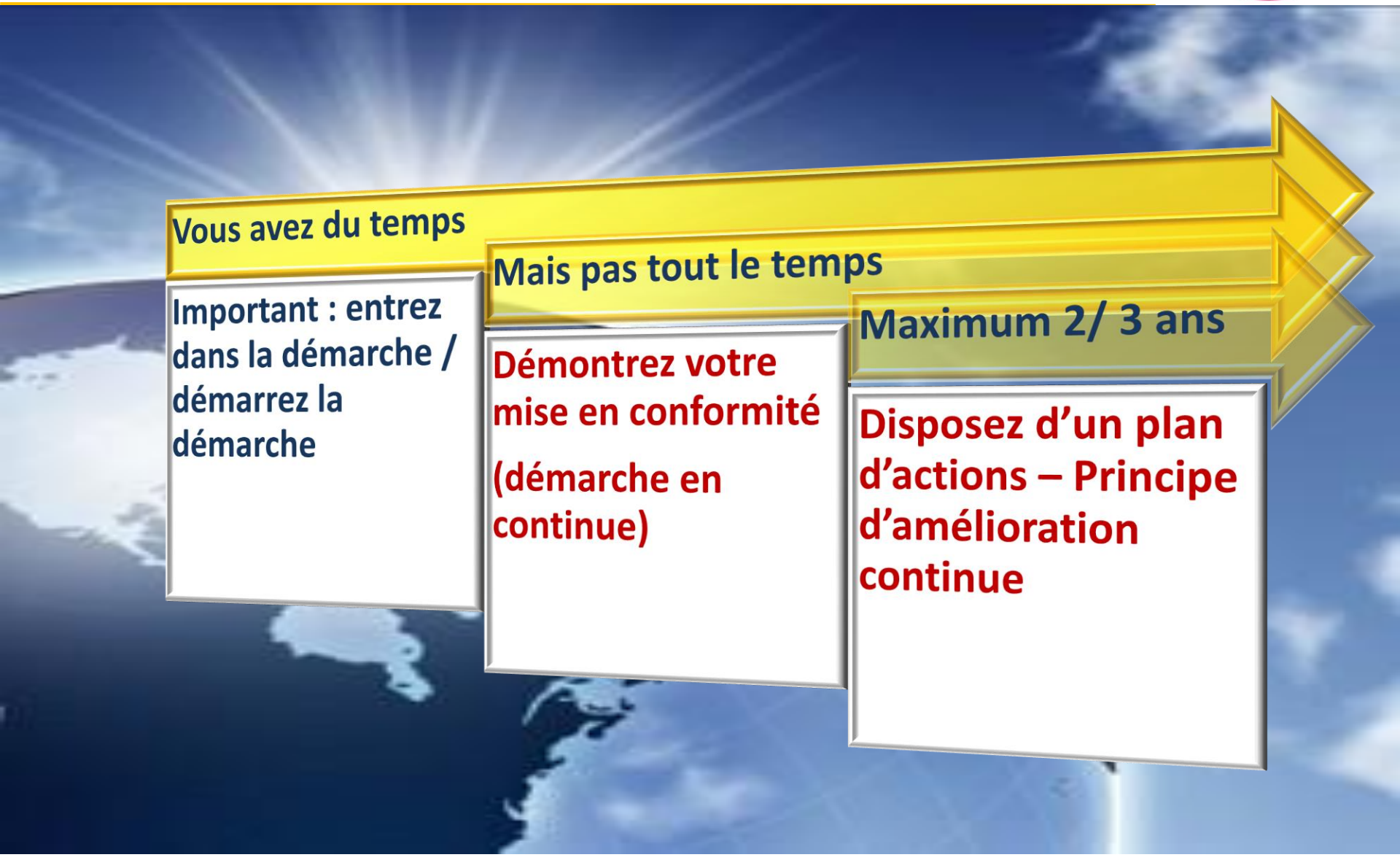
3 juillet 2018

CNEH
ÉCOLE DE RÉFÉRENCE
CONSEILLER DE CONFIANCE

Le RGPD après le 25 mai : avez-vous démarré votre mise en conformité ?

Intervenante :
Isabelle Génot Pok, Juriste consultante-formatrice, droit de la santé, CNEH

Le RGPD et VOUS…



1 Petits rappels sur le cadre juridique applicable

Petit rappel du nouveau cadre juridique de la protection des données personnelles

RGPD

Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Publication
27 avril 2016

Mise en œuvre par les acteurs de santé

RGPD
d'application
immédiate
25 mai 2018

Loi CNIL modifiée (V3)

Adaptation et compléments au RGPD (environ 50 marges de manœuvre)

+

Publication
20 juin 2018
On attend environ une dizaine de décrets…

Rappels sur les fondamentaux du RGPD

Champ d'application :

Le RGPD s'applique à **toutes les entreprises et établissements ou organismes établis sur le territoire de l'Union européenn**e, MAIS aussi **à tous ces acteurs hors UE** lorsqu'ils offrent des biens ou des services à des résidents de l'UE ou qu'ils **traitent des données** de résidents UE.

Les objectifs du RGPD :

- **Uniformiser** les politiques européennes en matière de protection des données / s'adapter notamment aux évolutions du numérique
- **Responsabiliser** les acteurs traitant des données personnelles
- **Protéger les personnes physiques** à l'égard des traitements de leurs données à caractère personnel
- **Donc renforcer** les droits des personnes
- **Étendre** le champ territorial
- **Crédibiliser la régulation** par une coopération renforcée entre les autorités
- **Apporter de la confiance** (espace de liberté, de sécurité et de justice) entre les acteurs pour le développement économique et le bien-être des personnes physiques

2 Points essentiels à toujours avoir à l'esprit

Les fondamentaux du RGPD

- **Données à caractère personnel** :

  Toute information se rapportant à une personne physique identifiée ou identifiable (art. 4 RGPD)

  - Est réputée être une « **personne physique identifiable** », une personne physique qui peut être identifiée **directement ou indirectement**, notamment :

Directement
exemple : nom, prénom

Indirectement
-avec une donnée par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique

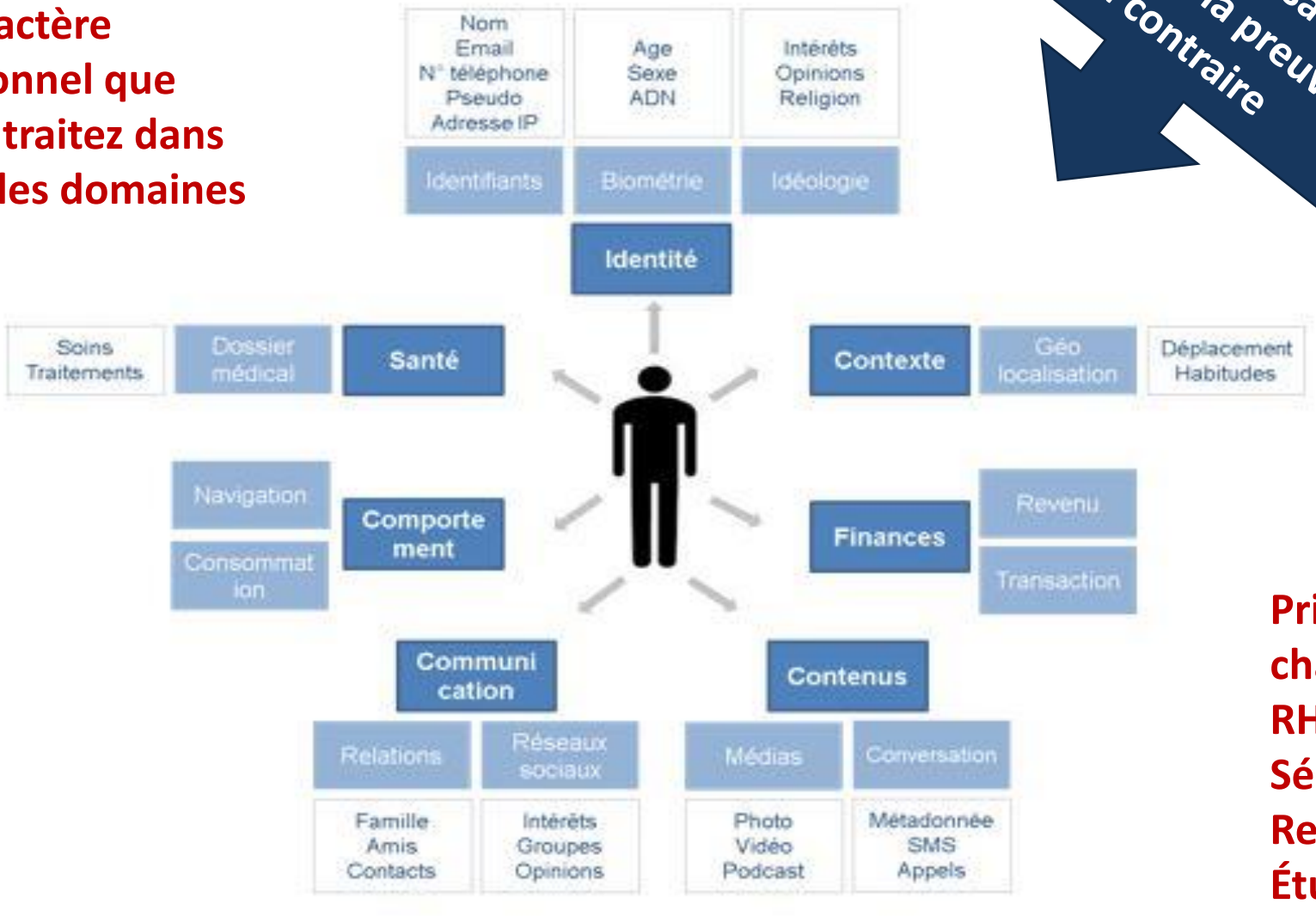
-avec plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image.

A partir du croisement d'un ensemble de données
– une femme vivant à telle adresse, née tel jour, abonnée à tel magasine et militant dans telle association, géolocalisation

Les fondamentaux du RGPD

Toute donnée est personnelle sauf à apporter la preuve du contraire

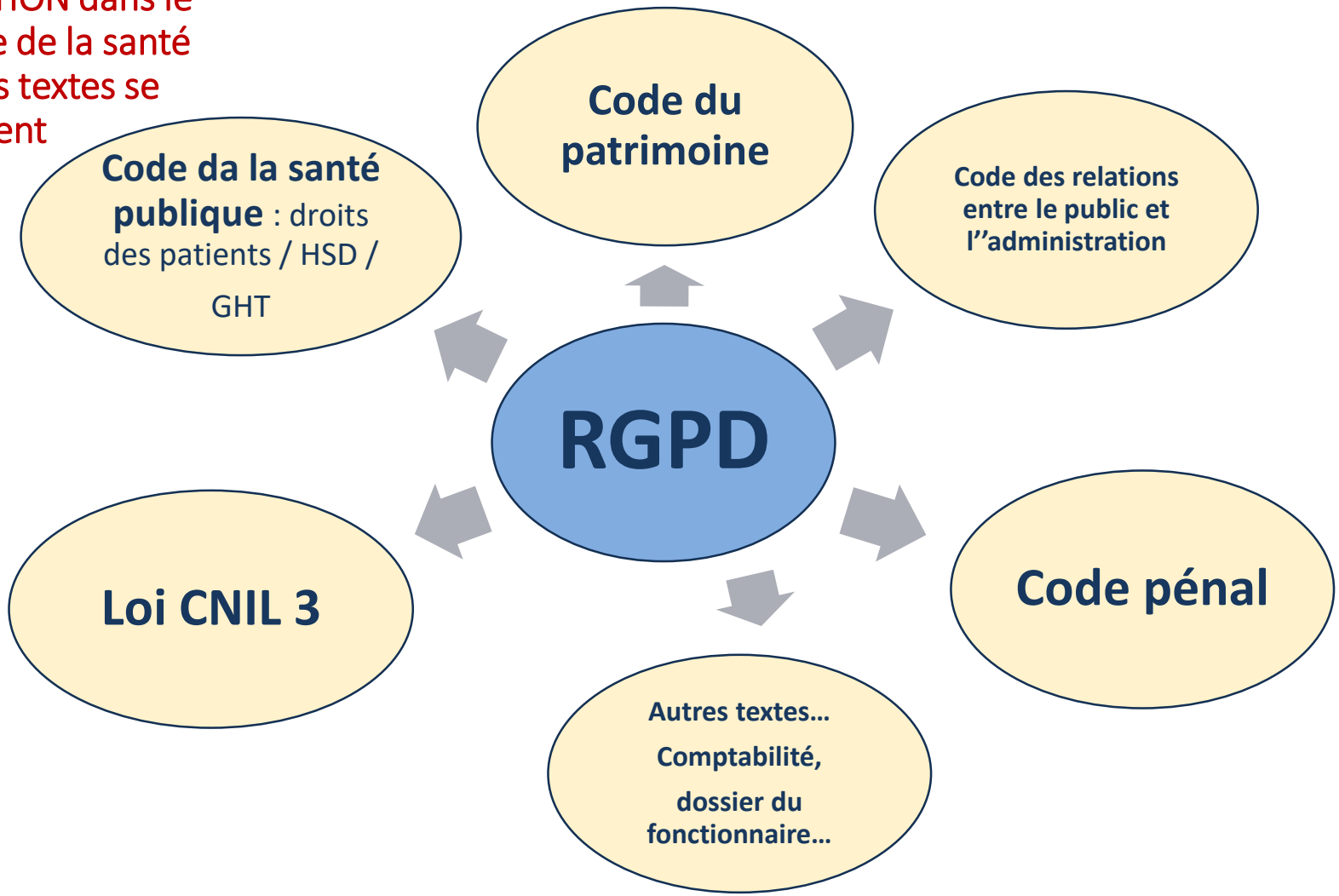
Les données à caractère personnel que vous traitez dans tous les domaines



Prise en charge
RH
Sécurité
Recherche
Études…

Les fondamentaux du RGPD

ATTTENTION dans le domaine de la santé plusieurs textes se conjuguent



Les fondamentaux du RGPD : Le renforcement des droits des personnes concernées

- Droit d'information (Art.13)
- Droit d'accès (Art.15)
- Droit de rectification (Art.16)
- Droit à la limitation de l'utilisation des données (Art.18)
- Droit à l'oubli (Art.17)
- Droit à la portabilité (Art.20)
- Le droit d'opposition (Art.21)
- Profilage (Art.22)
- Consentement (Art.7,…)
- Droit à réparation en cas de violation de données (Art.82)

Un élément fondateur du RGPD : rendre à la personne la maîtrise de ses données

Attention tous ne sont pas applicables tel quel aux EPS/EPMS

De plus: des droits qui se conjuguent avec d'autres textes

Les fondamentaux du RGPD

Moi **patient quels** sont mes droits ?

ATTENTION adaptez vos documents

- Droit à l'information — complexe
- Droit d'accès aux données
- Droit à réparation
- Le consentement au traitement — Sauf exceptions : traitements réalisés pour recherche
- Droit de rectification des données
- Droit à l'effacement (droit à l'oubli) — limité — Avec conditions
- Droit à la limitation du traitement — limité
- Droit à la portabilité
- Droit d'opposition — limité

Profilage !

Les fondamentaux du RGPD

Moi **agent public** quels sont mes droits ?

ATTENTION : adaptez aussi vos documents

Droit à l'information

Droit d'accès aux données

Droit à réparation

Le consentement au traitement

exceptions ex : badges self !

Droit de rectification des données

Droit à l'effacement (droit à l'oubli)

Avec conditions

limité

Droit à la limitation du traitement

limité

Droit à la portabilité

Droit d'opposition

limité

Données sensibles

Profilage

sans algorithme apprenant

Recommandations

- Réfléchir pour tous vos traitements aux droits impliqués
  - Se re-questionner // aux principes de licéité, minimisation, conservation, intégrité, exactitude..

- Soit créer des documents…
- Soit faire évoluer vos documents déjà existant sur les droits des usagers et des personnels au regard des obligations des établissements de santé et médico-social
  - Prévoir une procédure pour informer la personne
  - Prévoir les procédures pour les droits d'accès, de rectification,…
  - Revoir les cas de consentement / retrait de consentement, opposition visés par le CSP

Les fondamentaux du RGPD

- Nécessité de se prémunir contre les violations de données :

  - C'est 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;

    - **Dans vos établissements de santé ou médico-sociaux cette violation implique :**
      - **l'accès interne,**
      - **l'accès externe au système,**
      - **l'organisation prévue pour la protection de ses données.**

    - *Mais attente d'un décret suite de **LIL 3** qui en atténuerait les déclarations*

Les fondamentaux du RGPD

- **Le principe de l'accountability : D'une obligation de moyens à une obligation de résultat**
  - **Renforcer la responsabilité** des responsables de traitement de données (RT) et des sous-traitants (ST)
  - Mettre en œuvre des mesures techniques et organisationnelles (niveau de sécurité adapté au risque encouru)
  - Mettre en oeuvre les procédures internes
  - Démontrer la conformité à la règlementation : Documenter la conformité au RGPD

RGPD et GHT

Point de vigilance

L'établissement support du GHT peut agir en qualité de **sous-traitant** des autres membres du groupement

L'établissement support devra, selon le cas, être certifié **hébergeur** de données de santé

Les fondamentaux du RGPD

- **Les outils de l'accountability**

  - *Note de cadrage Conformité RGPD (conseil)*

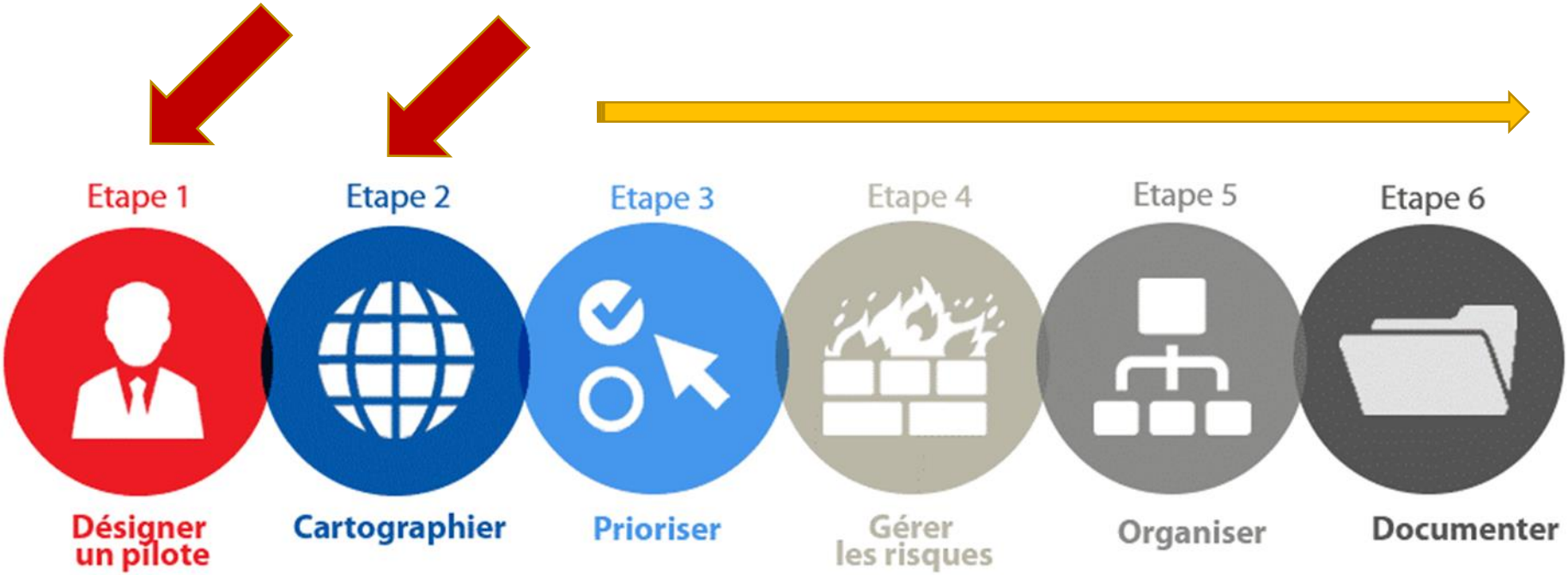
  - Registre des activités de traitement
  - Privacy by Design
  - Privacy by Default
  - Analyse d'impact (Private Impact Assessment - PIA)
  - Délégué à la protection des données (Data Protection Officer)
    - Désignation, Fiche de poste, Bilan annuel, Programme d'audits
  - Programme de sensibilisation au RGPD
  - Exigences vers les prestataires
  - Procédures de prise en compte des demandes des personnes
  - Procédure de notification d'incident

  - Etablir un lien avec les démarches de
    - Sécurité de l'information
    - Gestion des risques dans l'établissement

3 La démarche à engager

RGPD : la démarche de mise en conformité

➢ 6 étapes…

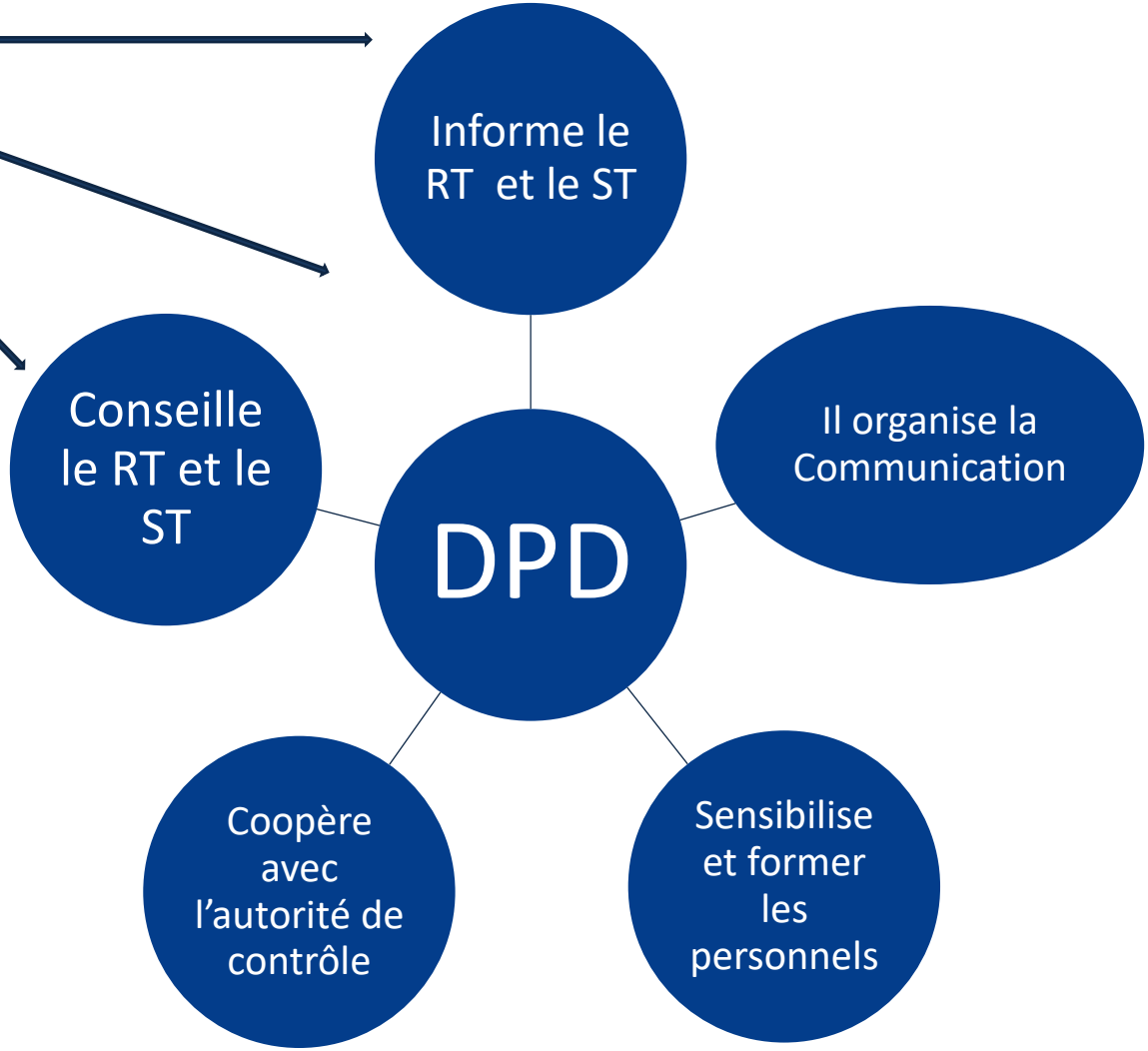


Nommer le Délégué à la protection des données /lettre de mission + fiche de poste

- Ses missions

+

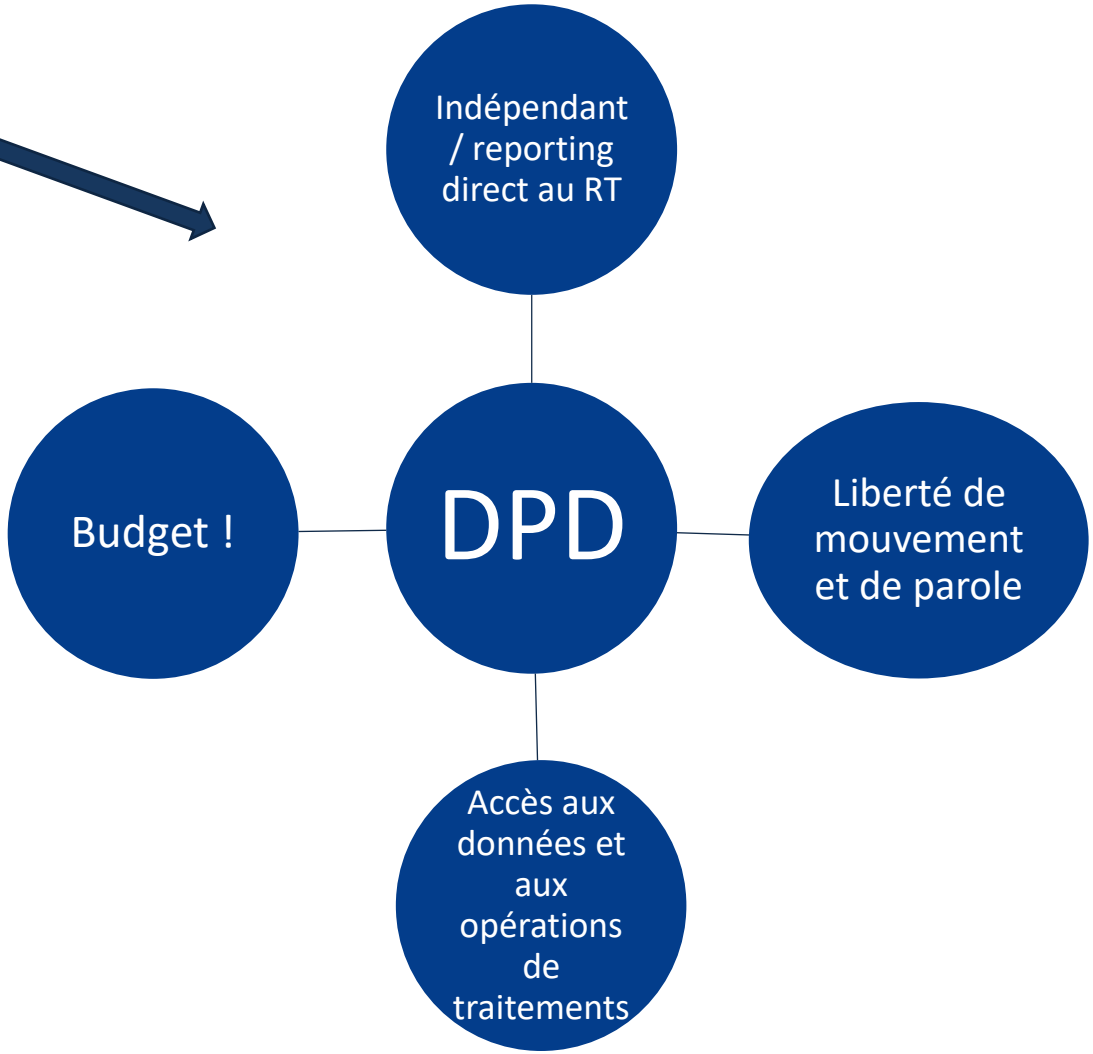
- Alerte des risques
- Supervise les audits
- Supervise les PIA
- Signale les violations de données
- Gère les demandes et réclamations relatives aux droits
- *+ rapport annuel*



Nommer le DPD

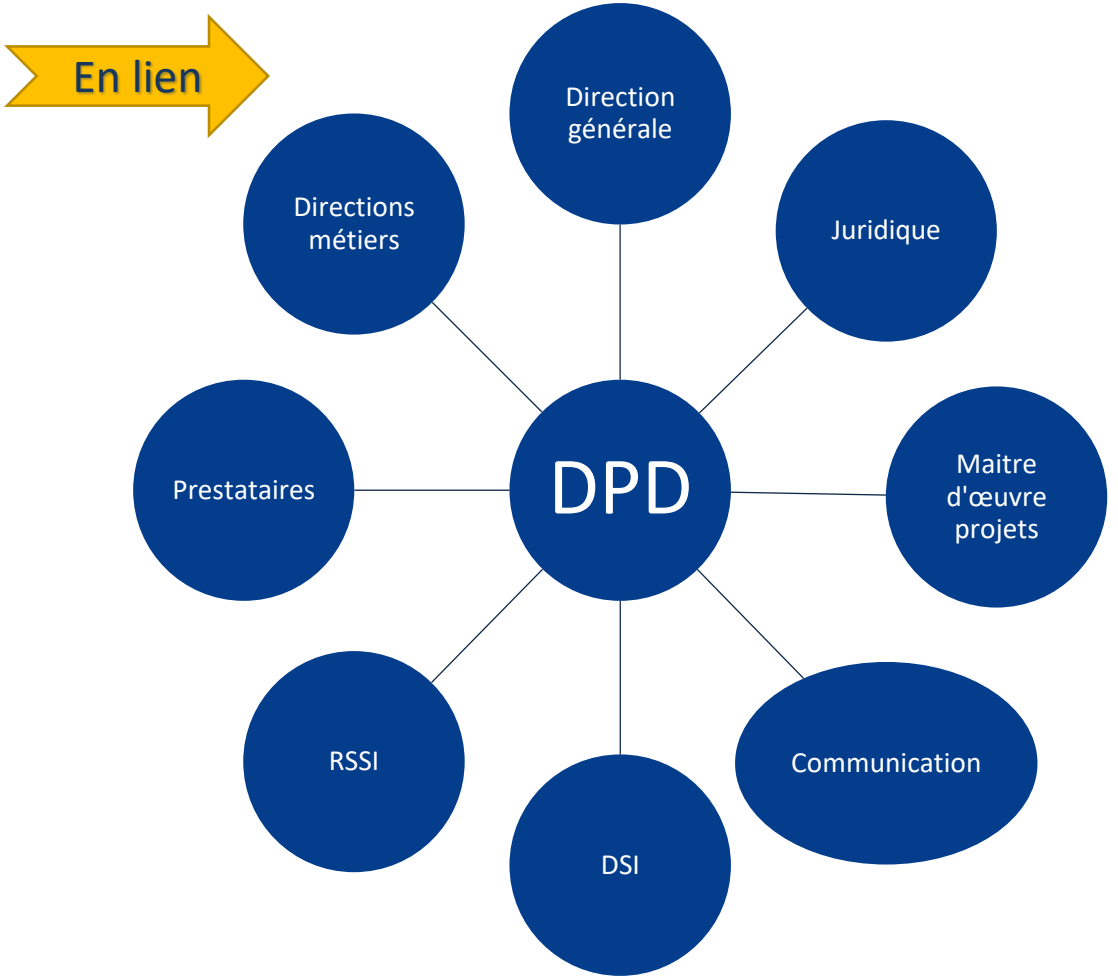
- Ses moyens

- **Si DPD mutualisé entre les membres du GHT**
  - → Garant de la mise en conformité pour le GHT
  - → Etablir une convention de service
  - → Chaque établissement déclare le DPD comme étant désigné par lui
    - Des référents relais dans chaque établissement si besoin



Nommer le DPD

- Est un Chef d'orchestre de la conformité au RGPD
- Doit être impliqué dans l'ensemble des activités de l'organisme, et en amont de tout projet
- Peut être
  - Interne à l'organisme, ou
  - Externe (mutualisation de la fonction = GHT)



Nommer le DPD

Trouver la bonne personne si ce n'est déjà fait

Qualités professionnelles

- Objectivité sens critique
- Crédibilité
- Diplomate
- Probité
- Confidentialité
- Communicant

Connaissances spécialisées

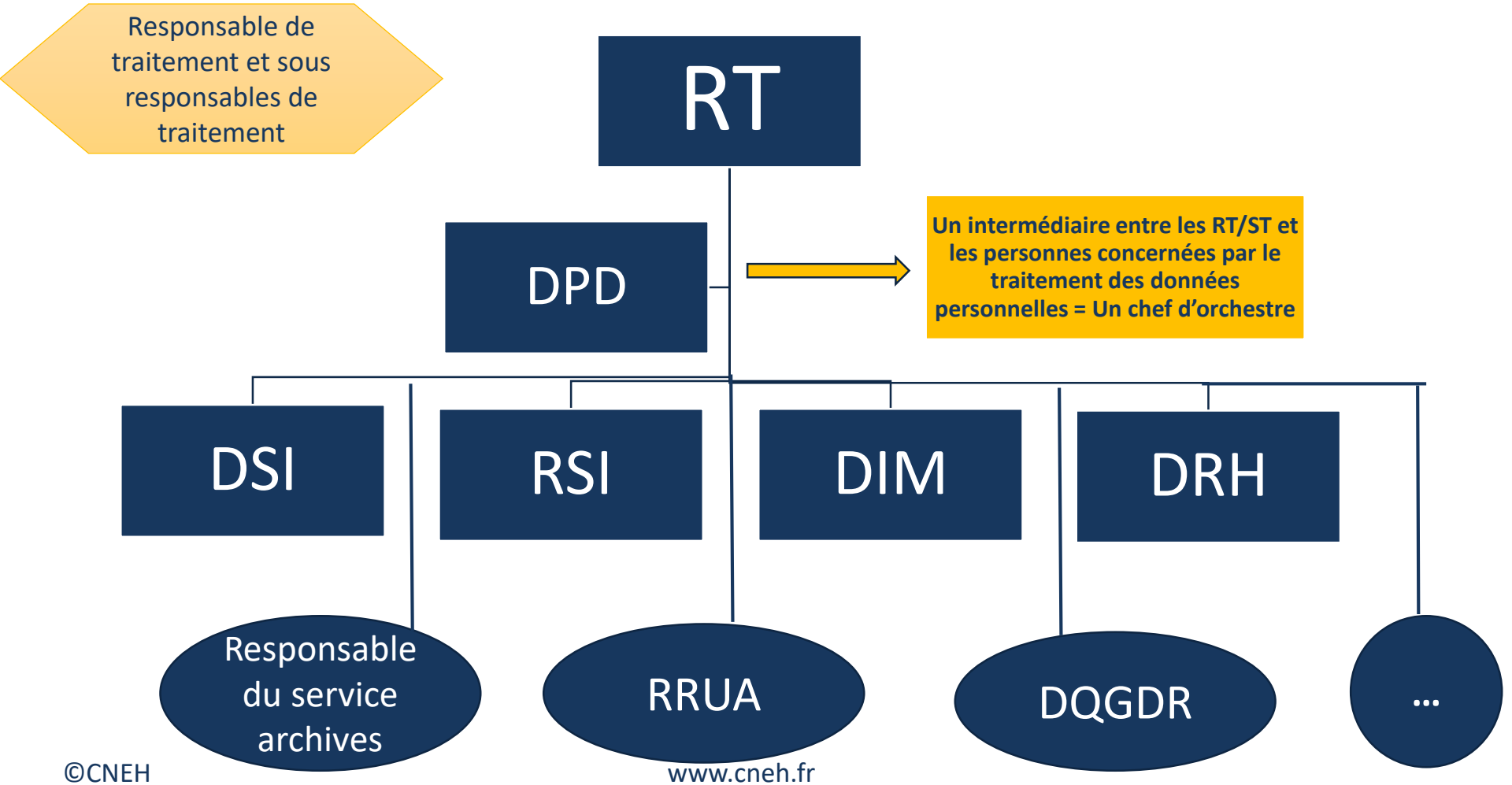
- juridiques
- techniques
- des pratiques en matière de protection des données
- Bonne connaissances du secteur d'activité

Capacité à accomplir ses missions

- Positionnement
- Indépendance
  - Ni un RT / direction
  - Ni un initiateur de traitement
- Disponibilité
  - DPD GHT !
- Avoir les moyens d'agir / réseau/relais/ …

Mise en place de la gouvernance de la protection des données

- **La gouvernance de la protection des données – Principe**



Vos outils de la mise en conformité

- **Note de cadrage Conformité RGPD**
  - Pas obligatoire
  - Conseillée pour initier le projet

SOMMAIRE

Vos outils de la mise en conformité

- **Cartographier vos traitements de données**
  - Recenser les services (tous les services)
  - Rencontrer les responsables opérationnels susceptibles de traiter des données personnelles
  - Lister tous les traitements existants par service
    - Les traitements sont identifiés par finalité (non par logiciel) : DPI/Recrutement/accès locaux…
    - Les « confronter » **aux conditions nécessaires** des traitements
    - **Faire le tri des traitements (données nécessaires ou pas)**
    - Lister les écarts entre les textes et la pratique
  - Constituer et renseigner le registre
  - → Devrait exister une cartographie des traitements du système d'information (sinon c'est l'occasion de le faire !) : base de travail / reprendre aussi ce que le CIL avait constituer

Petits rappels

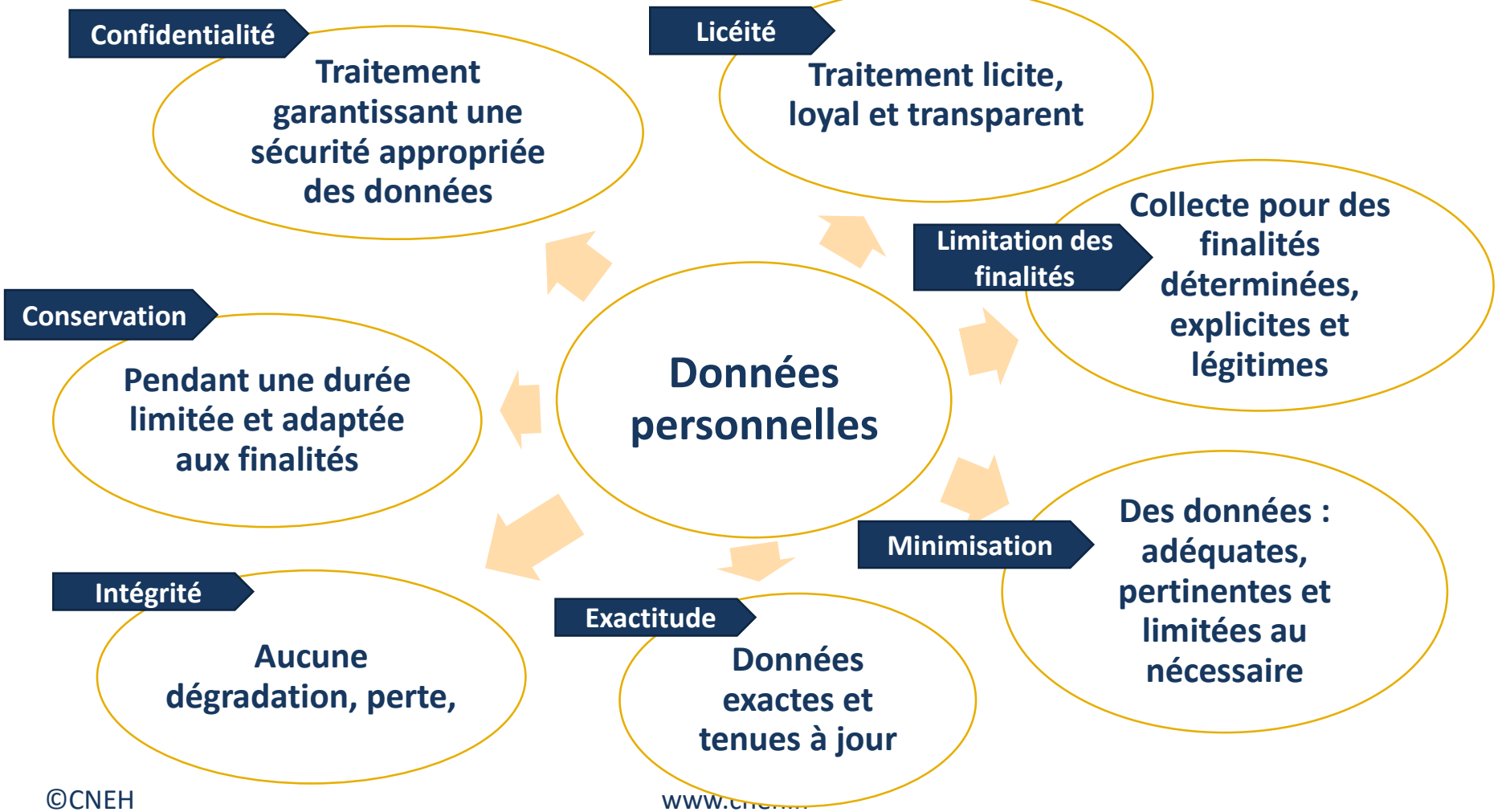
- **Un traitement :**
  - **Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés** et appliquées à des données ou des ensembles de données à caractère personnel, telles que :
    - la collecte, l'enregistrement,
    - l'organisation, la structuration,
    - la conservation,
    - l'adaptation ou la modification,
    - l'extraction, la consultation,
    - l'utilisation, la communication par transmission,
    - la diffusion ou toute autre forme de mise à disposition,
    - le rapprochement ou l'interconnexion,
    - la limitation, l'effacement, la destruction.

Vaut pour toutes les données quel que soit leur support

  - **Dans un système d'information, un traitement peut être représenté par un ou plusieurs logiciels, des fichiers xls,….**

Petits rappels

- Les principes à respecter pour chaque traitement (art.5 RGPD)



Vos outils de la mise en conformité

- **Constituer le registre des traitements de données**

Registre

S/ responsabilité du RT, même si tenu par le DPD

Nom / coordonnées de l'établissement

Nom/ coordonnées du DPO

Liste des activités de votre établissement

Registre tenu à jour de toute évolution de toute modification de chaque traitement

Pour chaque activité recensée

Création d'une fiche à tenir à jour :
-Recrutement
-Gestion de la paye
-Gestion des badges
-DIP…
la base juridique de l'opération de traitement doit être indiquée

Si vous êtes RT et ST
ex : en GHT -> conseil = 2 registres

Vos outils de la mise en conformité

- **A partir du registre et de la cartographie**
  - Identifier les risques et les gérer
    - une approche par risque doit être suivie pour identifier les priorités de la mise en conformité des traitements qui peuvent entrainer des risques élevés pour les personnes
  - Évaluer les écarts avec le RGPD = pour actions d'amélioration
  - Document de pilotage de la conformité
  - Tenu à la disposition de la CNIL en cas de contrôle

Vos outils de la mise en conformité

- L'audit organisationnel : contrôle des pratiques en matière de protection des données personnelles
  - Répartition des responsabilités dans l'organisation (DAF, DRH, DSI, …)
  - Formalisation de cette répartition (procédures, règles applicables …)
  - Objectif : adopter une **gouvernance** de la protection des données
  - S'assurer d'informer le DPD au début de chaque projet
  - Apporter la preuve de l'étude de conformité au RGPD

Vos outils de la mise en conformité

- **La sécurisation des systèmes d'information**
  - Garantir la protection des données (Privacy by Design et Privacy by Default – Art.25)
    - Dès la conception des produits ou services, systèmes d'exploitation des données à caractère personnel
    - Obligation de disposer d'une démarche de sécurité de l'information (confidentialité, intégrité, pérennité)
    - Garantir par défaut les seules données nécessaires traitées
    - Garantir le respect des droits des personnes
    - Créer un référentiel sécurité à jour
    - ….

Vos outils de la mise en conformité

- L'analyse d'impact (PIA)
  - Réaliser une analyse d'impact des opérations envisagées sur la protection des données personnelles (PIA / Privacy Impact Assesment)

En attente de la liste des types d'opérations de traitement = PIA requis

  - Permettre aux responsables de traitement et aux fournisseurs de solutions de pouvoir justifier du niveau de garantie proposée en termes de protections de données
  - Pour toutes activités qui peuvent avoir des conséquences importantes en matière de protection des données personnelles

Faire converger les **démarches** existantes

  - Prévoir des mesures afin de diminuer les conséquences sur les dommages potentiels // protection des données à caractère personnel
  - Consultation des autorités de contrôle avant toute mise en œuvre des ces activités (art. 35)

➢ Outil proposé par la CNIL (exemple)

Vos outils de la mise en conformité

- Les procédures internes
  - Charte informatique
    - Utilisateurs, administrateurs SI et référents applicatifs, prestataires
  - Politique de protection des données
    - À intégrer dans la PSSI
    - Enjeux pour l'organisme et règles à respecter
  - Sensibilisation et formation du personnel concerné
  - Déclaration d'un incident (violation des données)
  - Prise en compte des demandes de la personne (accès, modification,…)

Vos outils de la mise en conformité

- **Documenter**:
  - Pour prouver la conformité au RGPD, regrouper la documentation nécessaire.
  - Le dossier devra notamment comporter les éléments suivants
    - la documentation sur les traitements de données, le registre des traitements, les analyses d'impact (PIA)
    - l'encadrement des transferts de données hors UE : à voir !
    - l'information des personnes, les mentions d'information, les modèles de recueil du consentement des personnes,
    - les procédures mises en place pour l'exercice des droits
    - les contrats définissant rôles et responsabilités des acteurs
    - les contrats avec les sous-traitants
    - les procédures internes en cas de violations de données
    - les preuves que les personnes concernées ont donné leur consentement si requis

4 Quelles sanctions ?

Avant les sanctions possibles…

- La CNIL autorité de contrôle, vous accompagne :

  - Effectuer des contrôles : sur la base du programme annuel des contrôles, ou des plaintes reçues par la CNIL, …., ou pour faire suite à un précédent contrôle.

  - Les contrôles opérés auront essentiellement pour but, dans un premier temps, de conseiller, d'accompagner l'entrée dans la démarche de conformité, de faire comprendre les textes.
    - Attention : l'accompagnement n'est pas individualisé
    - **Attention à ce qui aurait déjà dû être fait antérieurement !!!!!**

Mais après cette période de clémence, il sera possible à la CNIL de prononcer des sanctions pour toute personne morale si celle-ci ne s'est pas conformée aux normes du RGPD

Sanctions possibles

- **Mise en demeure + délai**
  - Satisfaire aux demandes d'exercice des droits
  - Imposer de mettre en conformité les traitements visés
  - Imposer que l'établissement informe de ces sanctions les personnes concernées par les manquements ou la violation
  - Effacer, rectifier des données à caractère personnel ou limiter le traitement
  - Peut passer à des sanctions financières sans mise en demeure

- **Avertissement**
- **Complément de mise en demeure**
- Ou :
- **Rappel à l'ordre**
- **Injonction de conformité / astreinte possible 10 000 e/jr**
- **Limitation temporaire ou définitives**
- **Retrait de certification**
- **Injonction à l'organisme certificateur concerné de refuser une certif. ou de la retirer**

Sanctions possibles

- **Sanctions financières**

  - Vérification si infraction grave
  - Question du % du CA / Hôpital ?
  - + 11 critères : ex : violation délibérée / négligence / si avantages financiers tirés de la violation…
  - Qui doivent être effectives, proportionnées, dissuasives
  - Réajustement si besoin

Sanctions pénales qui demeurent après le 25 mai, et la loi CNIL 3

- Non-respect de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité : articles 226-17 et 226-17-1 du Code pénal / 300.000 euros d'amende et 5 ans d'emprisonnement
- Détournement de la finalité des données personnelles : article 226-21 du Code pénal / 300.000 euros d'amende et 5 ans d'emprisonnement

Faire pression par la dissuasion ..

6

A vous de construire votre feuille de route

Pour démarrer ….

- Désigner un DPO (interne, externe)
- Cartographier les services / les traitements
- Rencontrer les responsables opérationnels susceptibles de traiter des données personnelles
- Lister tous les traitements existants par services
  - Les « confronter » aux conditions nécessaires des traitements
  - Faire le tri des traitements
- Élaborer le registre et PIA
- Procédures ….
  - Avec le RSSI, le Responsable Qualité et Risques

Pour démarrer…

LE CERCLE VERTUEUX DU RGPD

- **Monitoring en Continu** des Traitements, Applications et Données à caractère personnel
- **Automatisation** des Contrôles et **Audit**

Traitements

- RH
- CRM
- Supply Chain
- Juridique
- Marketing
- Etc.

#1 Inventaire

- Collecte et corrèle les informations RH et données d'accès aux informations
- Automatise le nettoyage des données.

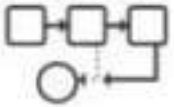
#2 Découverte

- Découvre les PII et leurs propriétaires
- Responsabilise les utilisateurs métier et les responsables d'applications dans le processus

#3 Contrôle

- Détecte les situations à risque
- Détecte les problèmes de qualité de données
- Identifie les causes,
- Orchestre les revues d'accès

#4 Correction



- Structure le Workflow
- Revue des accès
- Correction des anomalies.
- Self-service…

#5 Audit

- Audit des droits d'accès aux applications et PII,
- Automatise l'administration
- Responsabilise les utilisateurs métier

Alimentation du Registre et des systèmes d'IAM et ITSM

13

Des questions ?

Merci pour votre attention