Conformité RGPD de l'AP-HP : Présentation, contexte et plan d'actions

Donatienne Blin – DPO

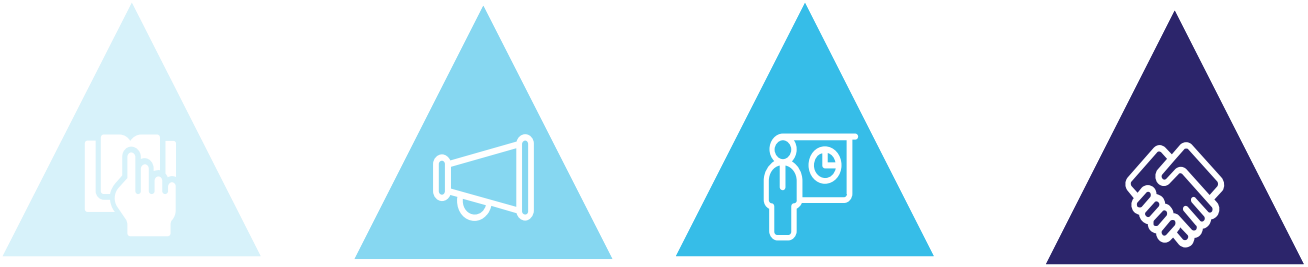
Commission Médicale d'Etablissement- Octobre 2021

1

Approche générale

- *Rôles et missions du DPO*
- *Le RGPD en synthèse*
- *Actualités et contexte 2020 /2021*

Rôles et missions du DPO : “Chef d’orchestre” de la conformité



Piloter

la conformité réglementaire et les chantiers

Contrôler

le respect de la réglementation

Informer et conseiller

l’organisme et ses employés

Coopérer

avec l’autorité de contrôle et être son point de contact

- Enjeux éthiques, rapport de confiance et vie privée
- Enjeux en terme d’image
- Enjeux liés à la continuité d’activité
- Enjeux financiers

Indépendance et absence de conflit d’intérêt

- ***Equipe dédiée :*** *4 personnes dans l’équipe DPO du siège et10 référents locaux ; équipe rattachée à la DSI et en lien fonctionnel avec la DAJ*
- ***Missions quotidiennes de l’équipe DPO :*** *conseils aux métiers (alertes et recommandations), revue de conformité (incluant les analyses d’impacts), rédaction & négociation des contrats, sensibilisation & formation, information des personnes, rédaction des procédures, gestions des formalités CNIL, réponses aux audits CNIL, traitement des plaintes CNIL et des demandes d’exercice de droits, inscription des traitements au registre…*

Le RGPD en synthèse : la protection des données personnelles

Définitions :

- ***Donnée personnelle*** *: toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement*
- ***Donnée de santé*** *: donnée relative à la santé physique ou mentale d'une personne qui révèle des informations sur l'état de santé*

Les principes fondateurs

- Finalités déterminées, explicites et légitimes
- Données pertinentes et proportionnées
- Durée de conservation limitée
- Sécurité et de confidentialité
- Respect des droits des personnes
- Transparence et accountability

Les droits RGPD des personnes :

Droit d'accès → Droit d'information → Droit d'opposition → Droit de rectification → Droit d'effacement

Adresse dédiée : *protection.donnees.dsi@aphp.fr*

Actualités et contexte 2020 /2021

CNIL.

Un contexte inédit….:

- Années 2020 et 2021 marquées par la crise sanitaire
- Volumétrie toujours croissante des projets en parallèle
- AP-HP au cœur de l'actualité Covid
- Protection des données de santé au cœur de toutes les réflexions
- AP-HP sous pression de la CNIL depuis le début de la crise sanitaire du fait :
  - Du caractère stratégique des SI nationaux gérés avec les partenaires publics
  - De la sensibilité des données traitées
  - Du volume de personnes concernées

… qui implique un nombre d'audits inédit :

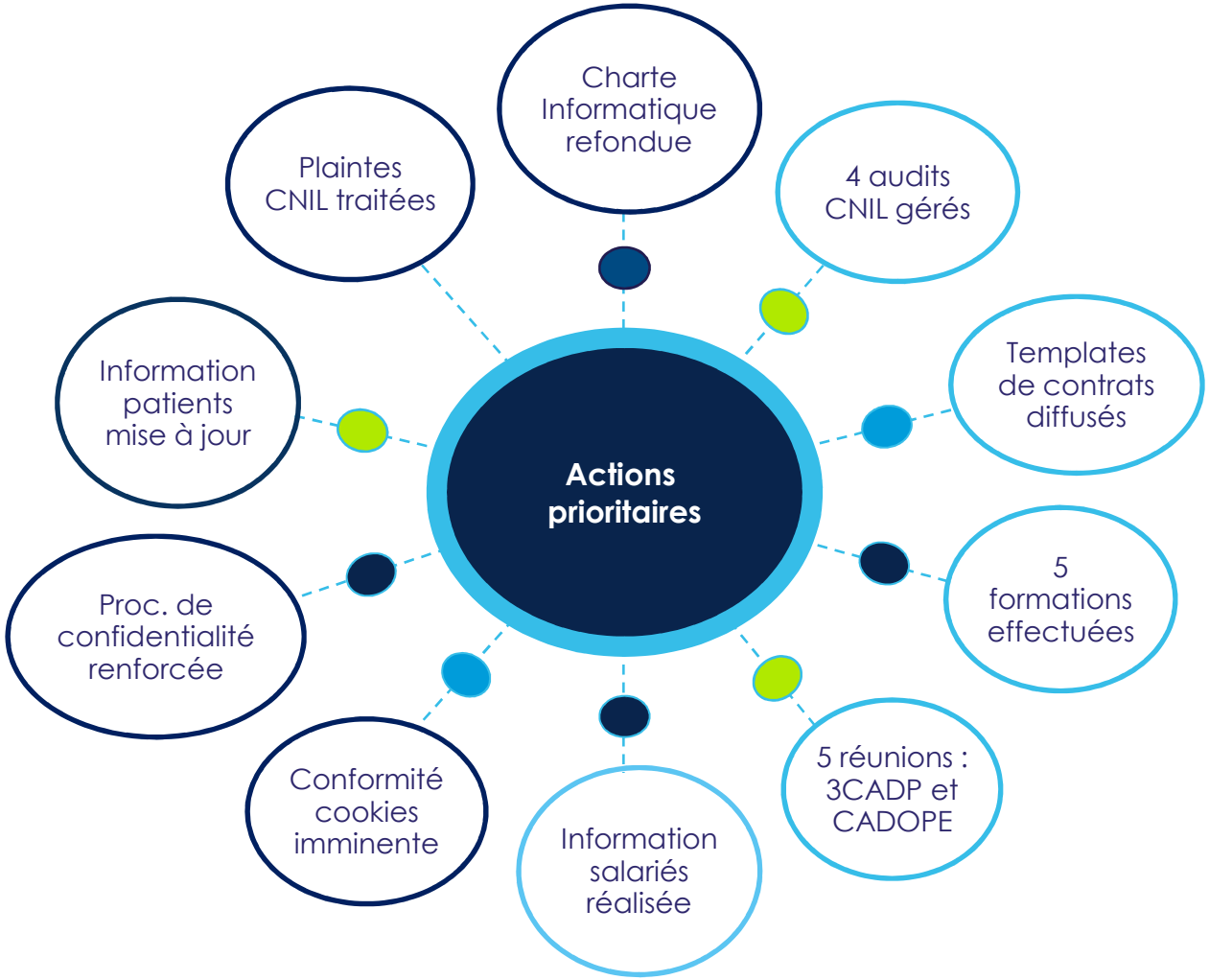
- Audits CNIL sur SIDEP tous les 3 mois - nouvel audit à venir suite à la violation
- Audit CNIL sur Orbis :
  - ✓ *« Mise en œuvre d'une mise à jour systématique des droits/habilitations »*
  - ✓ *« Mise en œuvre d'un système de surveillance de l'utilisation du mode bris de glace »*
  - ✓ *« Limiter la visibilité des dossiers administratifs par les agents administratifs aux seuls patients admis dans l'établissement dans lequel ils exercent »*
  - ✓ *« Journaliser l'ensemble des accès aux données médicales y compris à celles se trouvant dans les agendas »*
- Audit CNIL sur Covidom / Covisan
- Audit CNIL des centres de vaccination AP-HP

2

Chantiers de la conformité

- *Etat des lieux à mi septembre 2021*
- *Les chantiers de la conformité*

Etat des lieux : priorités traitées depuis janvier 2021



Chantiers prioritaires restant à mener :

- **Chantier "Sensibilisation, formation et communication" :**
  - ✓ Diffusion large des bonnes pratiques = sensibilisation au jour le jour, communication à tous via tout canal
  - ✓ Formations de tous les métiers = chantier formation DSI et URC débutent en octobre 2021
  - ✓ Expertise des référents DPO locaux à renforcer = poursuite des formations initiées

- **Chantier "Gouvernance et procédures" :**
  - ✓ Revue des process pour plus d'efficacité et de protection des droits des personnes = identification, audit et optimisation des procédures existantes, outils pédagogiques
  - ✓ Réorganisation/ renforcement de la relation avec la CNIL = moins d'audits, plus de conseils
  - ✓ Audits et application des sanctions en cas de violation du secret medical = plus de contrôles et de suivi

- **Chantier "Cartographie et conformité des traitements":**
  - ✓ Mise en conformité des traitements / projets passés = audits des traitements (revue de conformité) contract management et mise à jour du registre
  - ✓ Contrats à revoir / avenantiser
  - ✓ Durée de conservation des données