adapei am

Association Départementale des Parents et Amis de Personnes Handicapées Mentales des Alpes-Maritimes

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

JOURNEE NEXEM SUR LES ENJEUX DU NUMERIQUE 19-03-2018

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

- **<u>Le point de départ :</u>**
  - N'était pas la perspective de l'intégration du RGPD en droit français.
- **<u>Mais une réflexion prospective sur :</u>**
  - L'évolution du secteur médico-social
  - Les enjeux du numérique appliqués au secteur médico-social
  - La structuration des systèmes d'information
  - L'évolution des métiers et de la façon de les exercer
  - La protection des droits et libertés individuels face à la montée en puissance des traitements informatisés.
- **Et comment se structurer pour prendre en compte les pistes issues de notre diagnostic?**

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

- **Petite histoire d'un partenariat gagnant-gagnant :**
  - Une préoccupation de fonds partagée avec la FONDATION de NICE, intervenant dans le champ social.
  - Au-delà d'une maturité différente des deux entités sur le sujet, le choix de s'allier pour établir un dossier de consultation conjointe sur les problématiques d'informatique et libertés en octobre 2016.
- **Autour de 3 objectifs :**
  - Diagnostic de conformité au regard des dispositions réglementaires en matière d'informatique et libertés.
  - Propositions de plan d'actions en vue du traitement d'éventuels points de non-conformité.
  - Propositions de modalités de gestion continue de la conformité.

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

Pour l'ADAPEI AM

- **Les chantiers menés en parallèle :**
  - Refonte de l'infrastructure support en matière de TIC.
  - Déploiement d'office 365 et de logiciels collaboratifs.
  - Reconfiguration du support SI.
  - Définition d'une politique de cyber-sécurité.
  - Définition du SDSI 2018-2022.
  - L'ensemble conduit en mode projet collaboratif avec le corps de direction, les cadres pilotes de projet sur des applications spécialisées, les référents qualité.

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

Pour la réalisation de la mission de conformité IL, suite à l'appel d'offres notre choix s'est porté sur RESSOURCIAL :

- C' est un Groupement Social de Moyens (art. 261 du CGI) sans but lucratif dédié au partage de ressources en Systèmes d'Information entre organismes gestionnaires du secteur social et médico-social. A ce titre, il conduit des diagnostics et audits au sein des structures pour évaluer leurs systèmes d'informations sous toutes leurs dimensions (organisation, infrastructures IT, circulation de l'information, ressources humaines, outils de gestion…). Ces actions comportent de manière générale un audit spécifique des dispositions prises en matière de protection des données personnelles et conduisent à des préconisations de mise en conformité avec les dispositions législatives et règlementaires.
- Ressourcial était conseiller de la FEGAPEI devenue NEXEM pour le service qualité pour lequel la protection des données personnelles est une des problématiques.

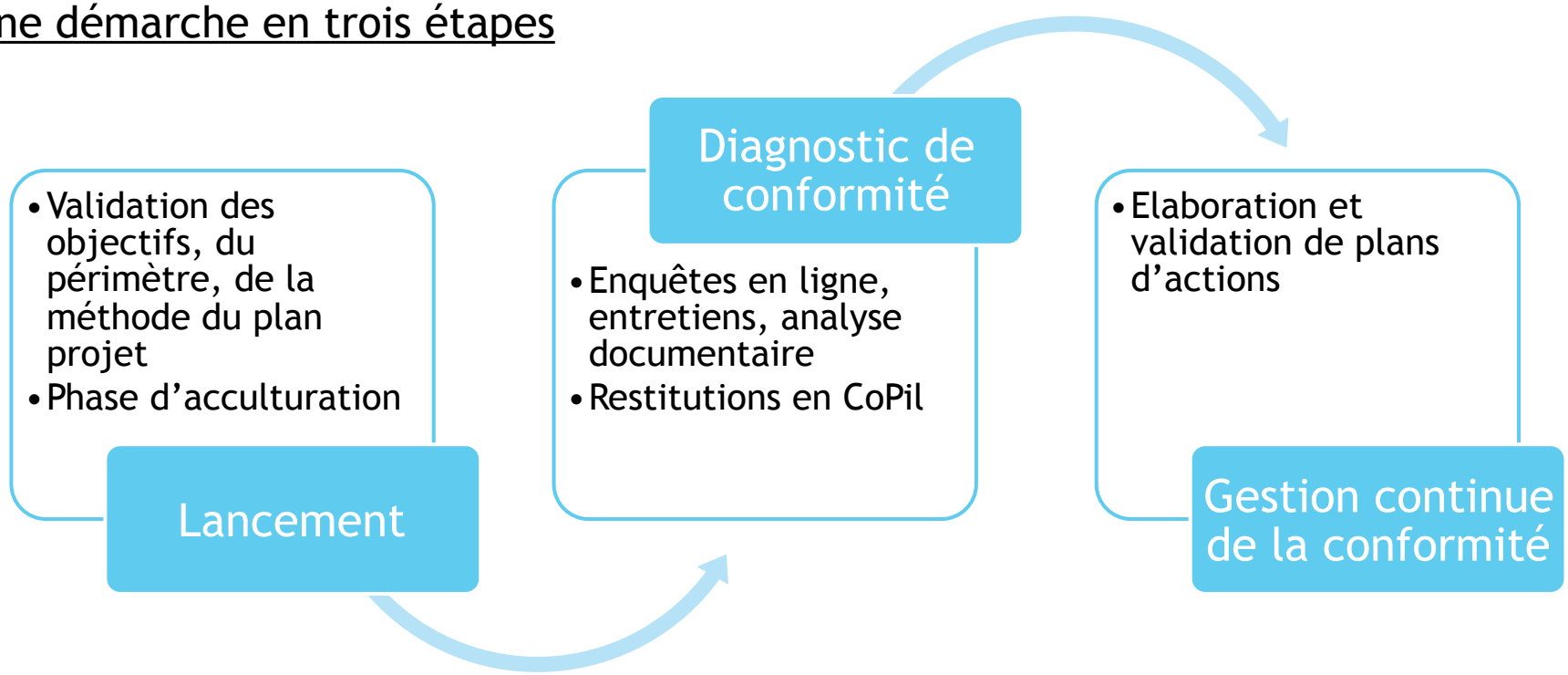
LE PÉRIMÈTRE DE L'ÉTUDE

Le périmètre de l'étude a été défini par :

- Les données à analyser
  - Données liées aux personnes accompagnées
    - Données liées à l'accompagnement
    - Données liées au soin et au dossier médical
    - Données administratives
  - Données liées aux salariés
    - Données administratives
    - Données liées au parcours professionnel
    - Données liées à l'organisation des services
    - Données liées aux autres tiers : adhérents, clients fournisseurs etc.
- Les process associés aux données
  - Acquisition des données
  - Flux internes
  - Flux externes

LA DÉMARCHE

- Dès le départ la perspective de l'application du RGPD a été prise en compte.
- <u>Une démarche en trois étapes</u>



- **Soutenue par un comité de pilotage dédié comprenant le DG et les Directeurs de territoire, une délégation du corps de direction, des personnes ressources issues de l'encadrement et une stratégie de communication dédiée.**

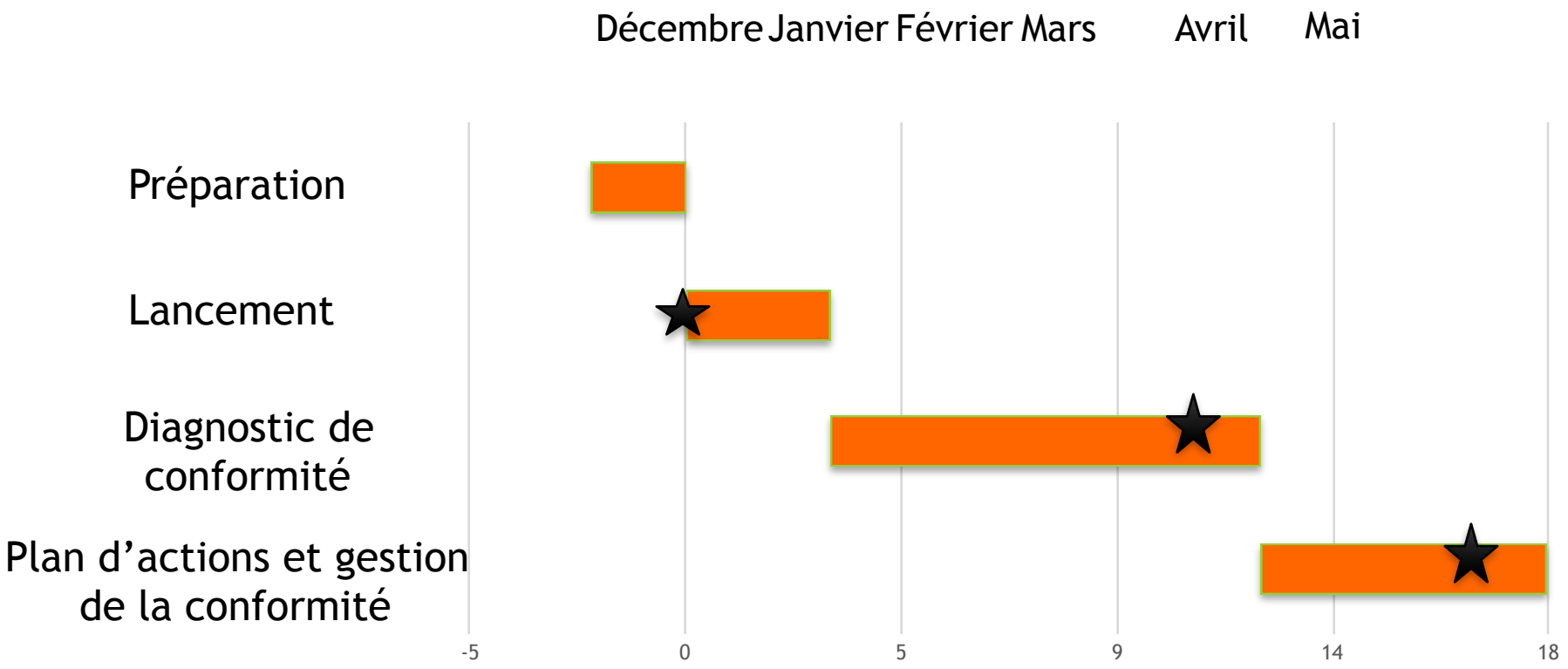
ORGANISATION

- Pour des raisons de simplicité, l'instance de décision a été limitée au seul Comité de Pilotage.
- La composition proposée doit être validée conjointement avec le prestataire retenu.
- Pour favoriser la fluidité et l'efficacité des travaux, les consultants doivent pouvoir agir transversalement tout en rendant compte si nécessaire.
- Ceci pourra s'avérer indispensable dans les cadre des questionnaires à questions fermées.
- La validation des enquêtes est un point important de même que la définition du panel des personnes qui seront interviewées, la préparation et le séquencement des entretiens.

FACTEURS CLÉS DE SUCCÈS

- L’implication de la Direction.
- La disponibilité des acteurs conformément au planning établi.
- La volonté d’aller à l’essentiel.
- La sincérité des éléments fournis lors des entretiens et des questionnaires.
- La capacité à se remettre en cause : « jouer le jeu ».
- Pour tout cela, il est essentiel que la démarche soit présentée sous un angle positif d’aide à l’amélioration des pratiques professionnelles.
- Il faut donc définir une stratégie de communication adaptée.

MACRO PLANNING DE L'ANALYSE DE CONFORMITÉ



Comité de pilotage

Étape du projet en semaine

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

Juillet 2017 fin de la mission initiale de RESSOURCIAL :

- Proposition d'un plan d'action de déploiement de la conformité.
- Transformation du CoPil initial en instance de pilotage du déploiement et définition de la stratégie de déploiement.
- Identification de référents protection de données : extension des missions des référents qualité.
- Identification de relais en établissements : sur la base du volontariat.
- Définition des actions de formation pour les référents et relais.
- Déploiement d'un SHAREPOINT dédié en support.

PLAN D'ACTIONS

Tâche	Responsable	Échéance	Livrables
Volet Organisationnel			
Création d'une instance de pilotage de conformité Informatique et liberté	Directeur Général	Octobre 2017	
Formation des référents qualité	Référents qualité	Octobre 2017	Support de formation
Mise en place de relais dans les établissements	Référents qualité Chef de service	Janvier 2018	Fiche de poste Support de formation
Coordonner les actions du service informatique et des référents Informatique et Liberté - Définir une politique de sécurisation des données conformes aux recommandations de bonnes pratiques (modification des mots de passe, charte informatique…)	Référents qualité Responsable informatique	Novembre 2017	Charte informatique BYOD Fiches pratiques à communiquer
Coordonner les actions du service informatique et des référents Informatique et Liberté - Rédiger une procédure de signalement des violations de sécurité	Référents qualité Responsable informatique	Novembre 2017	Procédures à rédiger
Identifier le DPO	Directeur général	Avril 2018	

PLAN D'ACTIONS

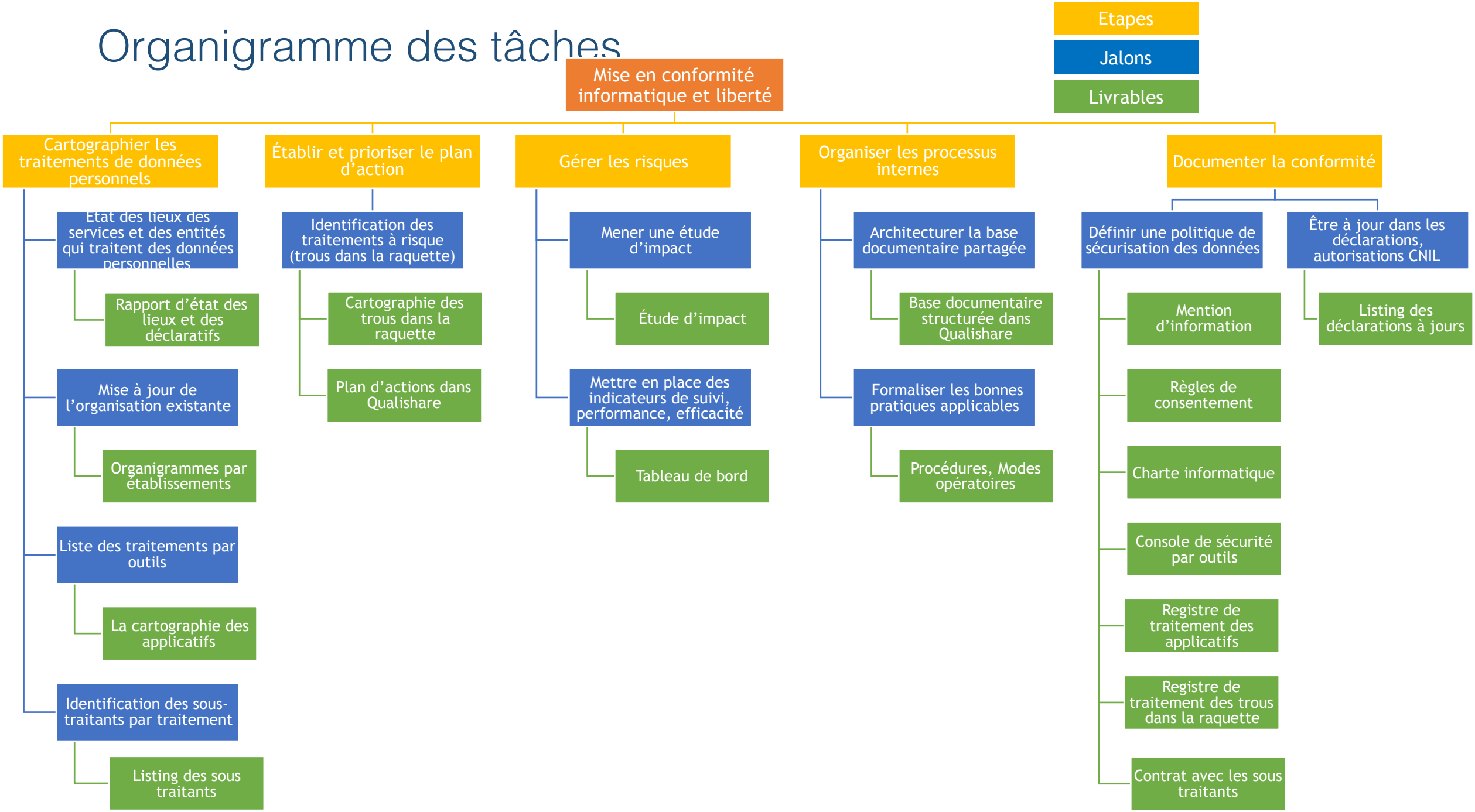
Tâche	Responsable	Échéance	
Volet Opérationnel			
Mise en place d'un outil dédié - base documentaire partagée	Référents qualité	Octobre 2017	Textes de loi et sites de veille
Rédaction de procédures et de documents socles	Référents qualité	Décembre 2017	Tableau des archives
États des lieux dans les établissements	Référents qualité	Mars 2018	
Déclarations auprès de la CNIL	Référents qualité en lien avec les référents du terrain	Mai 2018	Tutoriel de déclaration CNIL Tableau des déclarations à effectuer

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

Travaux en cours :

- Actualisation du règlement intérieur, rédaction d'une charte d'utilisation des nouvelles technologies de l'information et de la communication et de procédures associées.
- Constitution d'un espace dédié et d'un fonds documentaire dans le SharePoint qualité.
- Engagement des missions et travaux des référents et relais sur la base d'un plan projet de mise en conformité.
- Définition d'un plan de formation spécialisé pluriannuel pour l'ensemble des salariés.
- **L'ensemble des démarches entreprises concourrent à établir une présomption forte de mise en conformité même si tout ne sera pas conforme lors de l'entrée en vigueur du RGPD.**

Organigramme des tâches



RÔLES ET RESPONSABILITÉS

JALONS	RIL	Relais	COPIL	Directeurs	Salariés et adhérents
État des lieux des services et des entités qui traitent des données personnelles	C	R	IC	C	A
Mise à jour de l'organisation existante	C	R	IC	C	A
Liste des traitements par outils	R	A	IC	C	I
Identification des sous-traitants par traitement	R	R	IC	C	A
Identification des traitements à risque (trous dans la raquette)	C	R	IC	C	A
Mener une étude d'impact	R	A	C	C	I
Mettre en place des indicateurs de suivi, performance, efficacité	AR	R	CI	C	I
Architecturer la base documentaire partagée	R	A	IC	C	I
Formaliser les bonnes pratiques applicables	R	A	IC	C	I
Définir une politique de sécurisation des données	R	A	IC	R	I
Être à jour dans les déclarations, autorisations CNIL	C	R	IC	C	A

R - il réalise
A - il rend des comptes
C - il conseille
I - il est informé

GANTT

LIVRABLES	Prédécesseur	Durée en jours
1. Rapport état des lieux		56
2. Organigramme par établissements	1	14
3. La cartographie des applicatifs	1	28
4. Listing des sous traitants	1	7
5. Cartographie des trous dans la raquette	1, 2, 3, 4	365
6. Plan d'actions dans qualishare	1, 2, 3, 4	28
7. Étude d'impact	1, 2, 3, 4	49
8. Tableau de bord	7	21
9. Structuration base documentaire	6	15
10. procédure, mode opératoire, document de communication	6	168
11. Mention d'information	6	56
12. Règles de consentement	6	28
13. Charte informatique	6	168
14. Console de sécurité par outils	6	84
15. Registre de traitement des trous dans la raquette	5	83
16. Registre de traitement des applicatifs	6	112
17. Contrat avec les sous-traitants	6	56
18. Listing des déclarations à jour	6, 7, 8	21

Cf. annexes « réseau de tâche » et Gantt

TÉMOIGNAGE DE L'ADAPEI-AM RELATIF À LA PROTECTION DES DONNÉES

Question à court terme :

- Compte-tenu de nos choix d'organisation, quelle formule pertinente concernant la nomination d'un DPO ?

Vision à 2 ans :

- Projet finalisé : registre de traitement opérationnel et suivi, conformité avec la RGPD.
- Dynamique de processus et suivi autonome, gestion continue de la conformité.
- La dimension protection des données personnelles est intégrée dans les repères de bonnes pratiques professionnelles.
- Obtention label CNIL Gouvernance Informatique et Libertés ou de la certification AFNOR spécialisée.

DES QUESTIONS ?