La conformité aux lois et règlements sur la protection des données personnelles

Diagnostic, recommandations et gestion de la continuité

- Protection des données personnelles : contexte
  - La réglementation et ses évolutions
  - Les enjeux de la conformité
- Ressourcial accompagne votre mise en conformité
  - Le périmètre
  - La démarche
  - L'estimation
  - Références

La réglementation et ses évolutions

- Évolution récente de la réglementation notamment dans le secteur médico-social :
  - Loi pour une république numérique
  - Décret sur le partage d'information entre professionnel de santé et du secteur médico-social
  - Autorisations uniques de la CNIL
  - Loi de modernisation de notre système de santé
  - Ordonnances relative à l'hébergement de données de santé à caractère personnel et relative la force probante des documents en santé
- Application du règlement européen sur la protection des données en mai 2018

Le règlement européen sur la protection des données

- Il entrera en application le **24 mai 2018**.
- Un **règlement** (et non une directive) il est directement applicable sans transposition.
- Il renforce le **droit des personnes** :
  - consentement et transparence,
  - portabilité des données (récupération et réutilisation),
  - conditions particulières pour les mineurs (droit à l'oubli),
  - actions collectives,
  - droit à réparation.
- La protection des données dès la **conception** et **par défaut** (privacy by design)

RGPD : de nouveaux outils de conformité

- la tenue d'un **registre des traitements** mis en œuvre
- la notification de **failles de sécurité** (aux autorités et personnes concernées : assimilées à un EIG)
- la **certification** de traitements
- l'adhésion à des **codes de conduites**
- le **DPO** (délégué à la protection des données)
- les **études d'impact** sur la vie privée (EIVP)
- **La preuve de la protection incombe à l'organisation gérante des données**, ce qui implique un documentation complète sur les moyens mis en œuvre pour assurer cette protection (accountability)

Des contraintes nouvelles : les autorités de protection peuvent notamment

- Prononcer un **avertissement** ;
- **Mettre en demeure** l’entreprise ;
- **Limiter** temporairement ou définitivement un traitement ;
- **Suspendre** les flux de données ;
- **Ordonner** de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la **rectification**, la **limitation** ou l'**effacement** des données ;
- Sanctions économiques accrues : **jusqu’à 4% du chiffre d’affaire** de l’entreprise

L’enjeu de la conformité

- Sensibiliser les équipes sur le respect des droits des usagers en matière d’information sur leur accompagnement
- Adopter les bonnes pratiques de sécurité au sein du système d’information
- Identifier les outils respectueux des droits fondamentaux
- Offrir les ressources nécessaires aux équipes sur les questions de confidentialité et de respect de la vie privée
- Anticiper les évolutions de la réglementation
- Assurer une conformité pérenne et la documenter

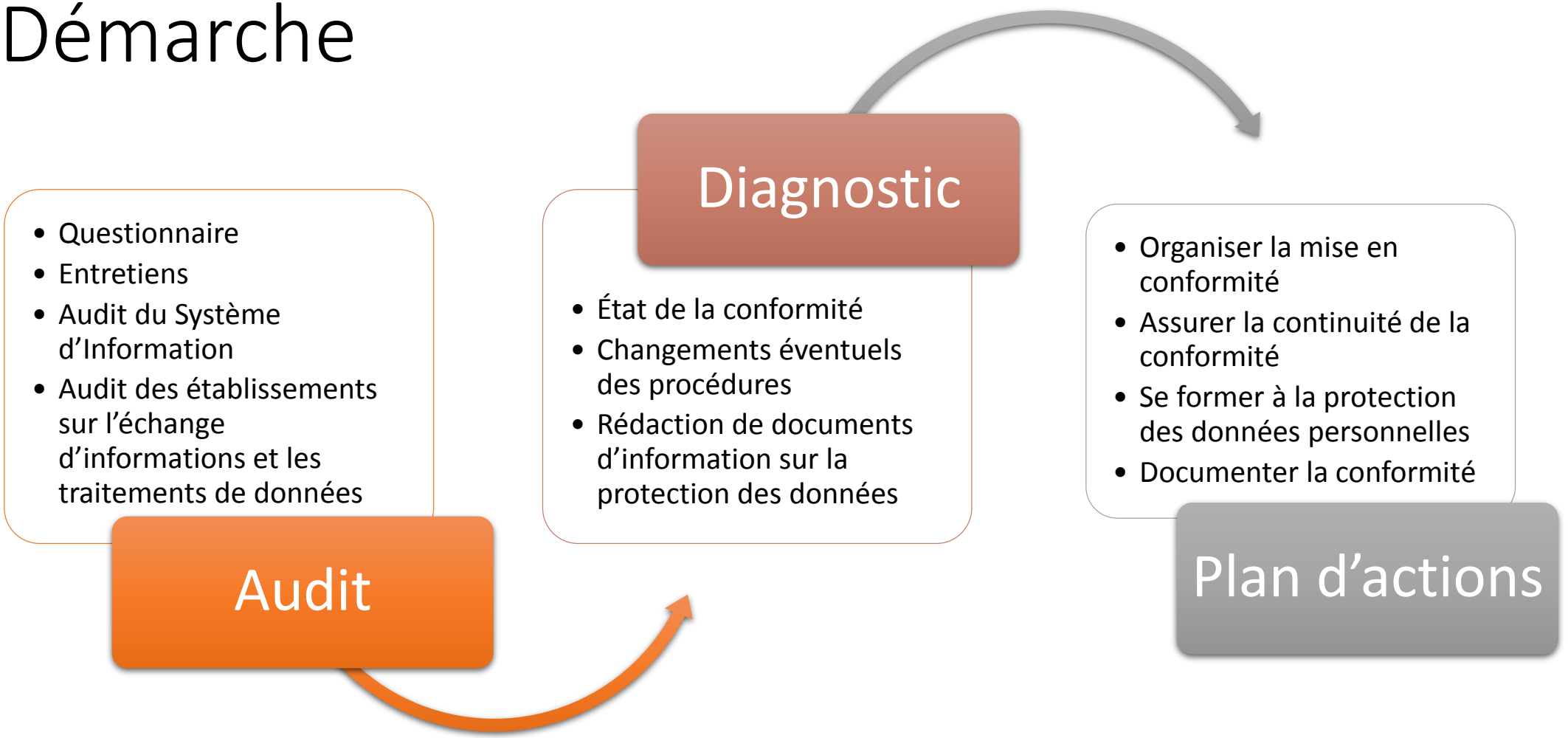
- Le Contexte de l’audit
  - La réglementation et ses évolutions
  - Les enjeux de la conformité

➢ Ressourcial accompagne votre mise en conformité
  - Le périmètre
  - La démarche
  - L’estimation
  - Nos références

Périmètre

- L’ensemble des données à caractère personnel :
  - sous format papier
  - sous format numérique
- L’ensemble des données à caractère personnel concernant :
  - Les personnes accompagnées
  - Le salariés
  - Les adhérents
  - Les bénévoles
- Les processus associés aux données :
  - Production
  - Gestion
  - Partage

Démarche



La démarche est conduite en mode projet et donne lieu à une validation à chaque étape.

Audit et diagnostic

- Objectifs :
  - Fournir une vision de l'état actuel de l'association vis-à-vis de sa conformité à la réglementation en vigueur et de l'intégration de bonnes pratiques
  - Communiquer sur la démarche auprès des professionnels
  - Permettre d'établir un plan d'action cohérent avec l'état de la conformité

- Outils :
  - Prise en compte des documents et démarches engagées
  - Questionnaire
  - Entretiens d'un panel de salariés représentatifs sélectionnés par l'association
  - Entretien et vérification du Système d'Information
  - Documents de recueil du consentement existants

- Livrables :
  - Rapport de conformité
  - Support de communication

Plan d'action de la conformité

- Objectifs :
  - Mise en conformité réglementaire et de sécurité
  - Adaptation des outils et des procédures
  - Acculturation des professionnels
  - Identification d’un DPO et organisation interne de maintien de la conformité

- Axes de l'élaboration de plans d’action :
  - Prioriser les actions à mener
  - Gérer les risques sur les données personnelles
  - Documenter les moyens de sécurisation des données (accountability)
  - Communiquer, former et informer les professionnels
  - Structurer la continuité de la démarche

- Livrables :
  - Plans d'actions
  - Ressource documentaire
  - Evaluation de la mise en œuvre, des effets et de la mise en oeuvre

Estimation du nombre de journées d'intervention

Étapes	Taches	Consultant		Sur site	Total
		Expert PDD	Expert SI		
Lancement	Réunion de lancement, rédaction d'un compte-rendu et d'un relevé d'actions	1	1	2	
Diagnostic de conformité	Entretiens avec questionnaire ouvert (hypothèse de 15 entretiens)	1	1	2	
	Diffusion, gestion et analyse du questionnaire à questions fermées	2	1		
	Analyse du volet « conformité RGPD »	3	0	0	
	Analyse du volet du système d'information	0	2	1	
	Comité de pilotage	1	1		
	Total de l'étape	8	6	5	
Plans d'action Gestion continue de la conformité	Formalisation des plans d'actions	3	1		
	Comité de pilotage	1	1	2	
	Total de l'étape	4	2	2	
Total général		**12**	**8**	7	**20**

Évaluation des charges

- La journée de prestation est facturée en fonction du tarif Ressourcial en vigueur.
- Aux estimations définies ci-dessus s'ajoutent les frais de déplacement, de restauration et d'hébergements des intervenants (la facturation de ces frais ne pourra se faire que sur présentation de justificatifs).

Références

- Ressourcial 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. Ces audits s'appuient principalement sur des méthodologies d'enquête et d'entretiens compréhensifs auprès des acteurs (professionnels et usagers).
- Ressourcial a, lors des 2 dernières années, conduit plus de 25 actions de ce type auprès de ses adhérents.
- Récemment Ressourcial propose un audit spécifique dédié à la protection des données personnelles. Deux associations ont pu profiter de son expertise.