POLITIQUE RGPD APEAI OUEST HERAULT

SOMMAIRE

L’introduction d'une stratégie de mise en conformité avec le Règlement Général sur la Protection des Données (RGPD) est une étape essentielle pour toute organisation qui traite des données personnelles. En effet, le RGPD est une réglementation complexe qui impose des obligations importantes en matière de protection des données personnelles, et qui peut entraîner des sanctions financières importantes en cas de non-conformité. Il est donc crucial pour les organisations de mettre en place des mesures solides pour se conformer au RGPD et assurer une protection adéquate des données personnelles qu'elles traitent. Cette stratégie doit être élaborée avec soin et suivie avec diligence pour garantir une mise en conformité complète et efficace avec le RGPD. Dans ce contexte, l'association APEAI Ouest Hérault a élaboré une stratégie sur 3 ans pour intégrer le RGPD dans les établissements médico-sociaux et les pratiques de l'association. Cette stratégie détaillée comprend des actions concrètes à mettre en œuvre chaque année pour assurer une mise en conformité progressive et complète avec le RGPD, et assurer une protection adéquate des données personnelles.

Le choix d'élaborer cette stratégie sur 3 ans a été motivé par plusieurs raisons :

Le RGPD est un règlement complexe qui implique des changements significatifs dans les pratiques de traitement des données personnelles des organisations. Les organisations doivent mettre en place des processus solides pour s'assurer qu'elles respectent toutes les obligations imposées par le RGPD. La mise en place de ces processus peut prendre du temps, en particulier pour les organisations qui n'ont pas encore commencé leur mise en conformité. Le choix d'étaler cette stratégie sur 3 ans permet d'avoir un temps suffisant pour mettre en place toutes les mesures nécessaires.

Une mise en conformité précipitée peut entraîner des erreurs et des manquements. En établissant un plan sur 3 ans, l'association APEAI Ouest Hérault dispose d'un temps suffisant pour prendre en compte toutes les exigences et les spécificités de leur activité et des différentes réglementations applicables. Cela permet également de garantir que toutes les mesures mises en place sont bien réfléchies et adaptées aux besoins spécifiques de l'organisation.

Le RGPD impose des exigences strictes en matière de protection des données personnelles et les organismes de contrôle sont chargés de veiller à ce que ces exigences soient respectées. Le fait de suivre un plan d'action sur 3 ans permet de montrer aux organismes de contrôle que l'association APEAI Ouest Hérault prend la mise en conformité très au sérieux et qu'elle met en place toutes les mesures nécessaires pour assurer la protection des données personnelles.

I) Stratégie politique RGPD APEAI Ouest Hérault (3ans)

a) Étape 1 : Sensibilisation et formation (année 1)

La première étape consisterait à sensibiliser tous les employés de l'APEAI Ouest Hérault aux principes du RGPD et à la protection des données personnelles. Pour ce faire, nous organiserions des sessions de formation en ligne pour expliquer les exigences du RGPD et les implications pour l'association et les établissements médico-sociaux. Ces sessions seraient suivies de sessions pratiques pour apprendre à mettre en œuvre des pratiques de protection des données.

Nous mettrions également en place un système de suivi et de sensibilisation régulière pour garantir que tous les employés sont informés et maintenus à jour sur les pratiques de protection des données.

b) Étape 2 : Évaluation des risques et mise en conformité (année 2)

La deuxième étape consisterait à évaluer les risques pour la protection des données et à mettre en conformité les établissements médico-sociaux et les pratiques de l'association. Nous procéderions à une évaluation de tous les traitements de données personnelles effectués par l'APEAI Ouest Hérault et ses établissements médico-sociaux pour identifier les zones à risque.

Nous travaillerions en étroite collaboration avec des experts en protection des données pour élaborer des politiques et des procédures pour la gestion des données personnelles, y compris les mesures de sécurité appropriées, les clauses contractuelles types, et l'identification de la base légale du traitement des données personnelles.

Nous mettrions également en place un plan d'action pour la mise en conformité, y compris la mise en œuvre de mesures correctives pour toutes les zones à risque identifiées.

c) Étape 3 : Surveillance et amélioration continue (année 3)

La troisième et dernière étape consisterait à surveiller la conformité à long terme et à améliorer continuellement les pratiques de protection des données. Nous mettrions en place un système de surveillance pour garantir que les politiques et procédures sont mises en œuvre et respectées dans les établissements médico-sociaux et les pratiques de l'association.

Nous organiserions également des audits réguliers pour garantir que tous les employés sont conscients de la manière de gérer les données personnelles et de l'importance de la protection des données. Nous tiendrions compte des résultats de ces audits pour continuer d'améliorer nos pratiques.

Enfin, nous veillerions à ce que les employés soient informés des mises à jour et des modifications apportées au RGPD pour garantir que l'APEAI Ouest Hérault reste à jour et conforme aux exigences réglementaires en matière de protection des données.

En résumé, cette stratégie en 3 étapes vise à sensibiliser, évaluer, mettre en conformité, surveiller et améliorer continuellement les pratiques de protection des données personnelles dans les établissements médico-sociaux et les pratiques de l'association APEAI Ouest Hérault.

II) Stratégie Opérationnel :

a) Plan d'action :

a.1 Sensibilisation et formation (N+1)

- Premier trimestre : Identifier les besoins en formation et les sujets à aborder.
- Deuxième trimestre : Élaborer les sessions de formation pour les employés de l'APEAI Ouest Hérault.
- Troisième trimestre : Organiser les sessions de formation pour tous les employés.
- Quatrième trimestre : Élaborer un plan de suivi et de sensibilisation régulière pour garantir que tous les employés soient informés et maintenus à jour sur les pratiques de protection des données.

a.2 Évaluation des risques et mise en conformité (N+2)

- Premier trimestre : Évaluer tous les traitements de données personnelles effectués par l'APEAI Ouest Hérault et ses établissements médico-sociaux pour identifier les zones à risque.
- Deuxième trimestre : Travailler en étroite collaboration avec des experts en protection des données pour élaborer des politiques et des procédures pour la gestion des données personnelles, y compris les mesures de sécurité appropriées, les clauses contractuelles types, et l'identification de la base légale du traitement des données personnelles.
- Troisième trimestre : Mettre en œuvre les politiques et les procédures de protection des données personnelles dans les établissements médico-sociaux et les pratiques de l'association.
- Quatrième trimestre : Mettre en place un plan d'action pour la mise en conformité, y compris la mise en œuvre de mesures correctives pour toutes les zones à risque identifiées.

a.3 Surveillance et amélioration continue (N+3)

- Premier trimestre : Mettre en place un système de surveillance pour garantir que les politiques et procédures sont mises en œuvre et respectées dans les établissements médico-sociaux et les pratiques de l'association.
- Deuxième trimestre : Organiser des audits réguliers pour garantir que tous les employés sont conscients de la manière de gérer les données personnelles et de l'importance de la protection des données.
- Troisième trimestre : Tenir compte des résultats des audits pour continuer d'améliorer les pratiques de protection des données.
- Quatrième trimestre : Veiller à ce que les employés soient informés des mises à jour et des modifications apportées au RGPD pour garantir que l'APEAI Ouest Hérault reste à jour et conforme aux exigences réglementaires en matière de protection des données.

En mettant en œuvre ce plan d'action, l'APEAI Ouest Hérault sera en mesure de se conformer aux exigences du RGPD et de garantir que les données personnelles de ses patients et de ses employés sont protégées de manière adéquate.

III) Déploiement du plan d'action :

a) Sensibilisation et formation :

a.1 Identifier les besoins en formation et les sujets à aborder :

Objectifs :

- Comprendre les principes clés du RGPD et leur application dans les établissements médico-sociaux.
- Savoir comment identifier les données personnelles et les traitements associés dans les établissements médico-sociaux.
- Comprendre les droits des personnes concernées et les obligations de l'APEAI Ouest Hérault en vertu du RGPD.
- Savoir comment répondre aux demandes d'exercice des droits des personnes concernées.

Actions :

- Élaborer une liste de tous les employés de l'APEAI Ouest Hérault qui ont accès aux données personnelles.
- Évaluer le niveau de connaissances de ces employés sur le RGPD et la protection des données.
- Établir une liste des sujets à aborder lors de la formation, en fonction des besoins identifiés.
- Élaborer un plan de formation qui couvre tous les sujets identifiés.

a.2 Élaborer les sessions de formation en ligne pour les employés de l'APEAI Ouest Hérault

Objectifs :

- Offrir une formation pour les employés de l'APEAI Ouest Hérault.
- S'assurer que tous les employés ont accès à la formation
- Élaborer du contenu de formation qui est facile à comprendre et à suivre.

Actions :

- Identifier des experts en protection des données qui peuvent fournir des conseils et des informations pour le développement du contenu de formation.
- Créer un calendrier de formation pour tous les employés de l'APEAI Ouest Hérault.
- Mettre en place un système de suivi pour s'assurer que tous les employés ont suivi la formation.

a.3 Organiser les sessions de formation pour tous les employés :

Objectifs :

- Offrir une formation en personne pour les employés de l'APEAI Ouest Hérault qui préfèrent une approche en face à face.
- S'assurer que tous les employés ont suivi la formation.
- Donner aux employés l'occasion de poser des questions et de discuter de leurs préoccupations.

Actions :

- Organiser des sessions de formation en personne pour les employés de l'APEAI Ouest Hérault.
- Fournir une formation en ligne pour les employés qui ne peuvent pas assister à la formation en personne.
- Créer un calendrier de formation pour tous les employés de l'APEAI Ouest Hérault.
- S'assurer que tous les employés ont suivi la formation en mettant en place un système de suivi.

a.4 Élaborer un plan de suivi et de sensibilisation régulière :

Objectifs :

- S'assurer que tous les employés sont informés et maintenus à jour sur les pratiques de protection des données.
- Créer un environnement de travail où la protection des données est une priorité.

Actions :

- Élaborer un plan de suivi et de sensibilisation régulière qui comprend des rappels de formation, des sessions d'éducation continue et des discussions régulières sur la protection des données.
- Mettre en place un programme de sensibilisation des employés sur les risques liés à la protection des données et les mesures à prendre pour les éviter.
- Élaborer des guides de bonnes pratiques pour les employés afin de les aider à comprendre les risques de la protection des données et comment les éviter.
- Organiser des formations pour les nouveaux employés afin de les sensibiliser aux pratiques de protection des données dès leur arrivée.
- Mettre en place un système de veille régulière pour s'assurer que toutes les pratiques de l'APEAI Ouest Hérault sont conformes au RGPD et aux normes de protection des données.

Ces actions devraient permettre à l'APEAI Ouest Hérault d'intégrer le RGPD dans les établissements médico-sociaux et dans les pratiques de l'association au cours de la première année. Bien sûr, il sera important de continuer à surveiller et à améliorer ces pratiques au fil du temps pour rester conforme aux règles de protection des données.

b) Évaluation des risques et mise en conformité :

Objectifs : Évaluer les risques liés à la protection des données et mettre en place des mesures pour assurer la conformité avec le RGPD.

b.1 Plan d'action :

Évaluation des risques :

- Identifier les données personnelles collectées, traitées et stockées par l'APEAI Ouest Hérault, ainsi que les différents traitements réalisés sur ces données.
- Évaluer les risques liés à la protection de ces données, notamment en ce qui concerne leur confidentialité, leur intégrité et leur disponibilité.
- Identifier les risques spécifiques liés aux établissements médico-sociaux.

Mise en conformité :

- Mettre en place des politiques et des procédures pour assurer la protection des données personnelles, y compris des protocoles de sécurité appropriés.
- Mettre en place des processus de notification en cas de violation de données.
- Désigner un Délégué à la Protection des Données (DPD) pour superviser la conformité avec le RGPD.
- Mettre en place des contrats avec des sous-traitants pour s'assurer qu'ils respectent également les normes de protection des données.

b.2 Fiches opérationnelles :

Évaluation des risques :

- Constituer une équipe chargée d'effectuer une évaluation des risques et de documenter tous les résultats.
- Identifier les données personnelles qui sont traitées par l'association et les différents traitements effectués sur ces données.
- Évaluer les risques liés à la protection de ces données, notamment en ce qui concerne leur confidentialité, leur intégrité et leur disponibilité.
- Identifier les risques spécifiques liés aux établissements médico-sociaux.
- Documenter toutes les conclusions et les recommandations issues de l'évaluation des risques.

Mise en conformité :

- Mettre en place des politiques et des procédures pour assurer la protection des données personnelles, y compris des protocoles de sécurité appropriés.
- Nommer un Délégué à la Protection des Données (DPD) pour superviser la conformité avec le RGPD.
- Élaborer des contrats avec des sous-traitants pour s'assurer qu'ils respectent également les normes de protection des données.
- Mettre en place des processus de notification en cas de violation de données.
- Organiser une formation pour les employés sur les nouvelles politiques et procédures.
- Établir un plan d'action pour la mise en œuvre des politiques et des procédures.
- Réaliser des audits réguliers pour s'assurer que toutes les politiques et procédures sont correctement appliquées.

En mettant en œuvre ces actions, nous devrons être en mesure d'évaluer les risques liés à la protection des données et de se mettre en conformité avec le RGPD au cours de la deuxième année.

c) Surveillance et amélioration continue

Objectifs : Surveiller et améliorer continuellement les pratiques de protection des données pour garantir la conformité avec le RGPD.

c.1 Plan d'action :

Surveillance continue :

- Mettre en place un programme de surveillance pour s'assurer que toutes les pratiques de l'APEAI Ouest Hérault sont conformes aux normes de protection des données.
- Réaliser des audits réguliers pour s'assurer que toutes les politiques et procédures sont correctement appliquées.
- Mettre en place un système de veille pour rester informé des évolutions du RGPD et des pratiques de protection des données.

Amélioration continue :

- Mettre en place un processus de gestion des incidents pour traiter rapidement les violations de données.
- Évaluer régulièrement les politiques et procédures de protection des données pour identifier les lacunes et les opportunités d'amélioration.
- Organiser des formations régulières pour les employés afin de s'assurer que tous les membres de l'association sont au fait des pratiques de protection des données.

c.2 Fiches opérationnelles :

Surveillance continue :

- Mettre en place un programme de surveillance pour s'assurer que toutes les pratiques de l'APEAI Ouest Hérault sont conformes aux normes de protection des données.
- Réaliser des audits réguliers pour s'assurer que toutes les politiques et procédures sont correctement appliquées.
- Documenter toutes les conclusions et les recommandations issues des audits de conformité.

Amélioration continue :

- Mettre en place un processus de gestion des incidents pour traiter rapidement les violations de données.
- Évaluer régulièrement les politiques et procédures de protection des données pour identifier les lacunes et les opportunités d'amélioration.
- Mettre en place des plans d'action pour améliorer les pratiques de protection des données.
- Organiser des formations régulières pour les employés afin de s'assurer que tous les membres de l'association sont au fait des pratiques de protection des données.
- Réaliser des évaluations annuelles de la conformité avec le RGPD et mettre en place des plans d'action pour remédier aux lacunes identifiées.

En conclusion, cette stratégie globale pour intégrer le RGPD dans les établissements médico-sociaux et les pratiques de l'association APEAI Ouest Hérault sur trois ans est un plan d'action concret pour garantir la conformité avec le RGPD et protéger les données personnelles des personnes concernées.

La première année est consacrée à la mise en place d'une base solide pour la protection des données, en désignant un responsable de la protection des données et en mettant en place des politiques et des procédures pour la gestion des données.

La deuxième année est axée sur l'évaluation des risques et la mise en conformité, pour identifier les lacunes dans les pratiques de protection des données et mettre en place des mesures pour y remédier.

La troisième année est consacrée à la surveillance et à l'amélioration continue, pour s'assurer que toutes les politiques et procédures de protection des données sont conformes aux normes de protection des données et pour identifier les opportunités d'amélioration.

En mettant en œuvre cette stratégie globale, l'association APEAI Ouest Hérault sera en mesure de protéger les données personnelles des personnes concernées, de se conformer au RGPD et de démontrer son engagement envers la protection des données.

IV) Annexe 1 : Retroplanning de la politique RGPD APEAI Ouest Hérault

Année	Objectifs	Plan d'action	Délais
1	**Mise en place d'une base solide pour la protection des données**		
	Désigner un responsable de la protection des données		
	1.1. Identifier un responsable de la protection des données (DPD)	1 mois	
	1.2. Nommer le DPD	1 mois	
	Mettre en place des politiques et des procédures pour la gestion des données		
	1.3 Identifier correspondant informatique et liberté (CIL)	1 mois	
	1.4 Nommer les CIL par établissements	1 mois	
	1.5. Réaliser un inventaire des données collectées et traitées	2 mois	
	1.6. Élaborer une politique de protection des données	4 mois	
	1.7. Élaborer un plan de gestion des incidents	4 mois	
	1.. Élaborer une procédure pour répondre aux demandes d'exercice des droits des personnes concernées	4 mois	
	Réaliser des formations pour les employés		
	1.7. Organiser une formation initiale sur le RGPD pour tous les employés	6 mois	
	1.8. Organiser des formations régulières pour maintenir les connaissances des employés sur le RGPD	Annuelle	
	1.9. Sensibiliser les employés à la protection des données et à la sécurité de l'information	Annuelle	
	Total	12 mois	
Année	**Objectifs**	**Plan d'action**	**Délais**
2	**Évaluation des risques et mise en conformité**		
	Évaluer les risques pour la protection des données		
	2.1. Réaliser une évaluation des risques pour la protection des données	3 mois	
	Mettre en place des mesures pour se conformer au RGPD		

	2.2. Mettre à jour les politiques de protection des données en fonction des résultats de l'évaluation des risques	6 mois	
	2.3. Mettre en place des mesures de sécurité techniques et organisationnelles	9 mois	
	2.4. Mettre en place un registre des traitements	12 mois	
	Réaliser des formations pour les employés		
	2.5. Organiser une formation pour tous les employés sur les mesures de protection des données et de sécurité	9 mois	
	Total	12 mois	
Année	**Objectifs**	**Plan d'action**	**Délais**
3	**Surveillance et amélioration continue**		
	Mettre en place un programme de surveillance		
	3.1. Mettre en place un programme de surveillance pour surveiller les violations de données	3 mois	
	Évaluer les politiques et procédures de protection des données		
	3.2. Réaliser une évaluation annuelle des politiques et procédures de protection des données	Annuelle	
	3.3. Évaluer les pratiques de protection des données des fournisseurs et des sous-trait		
	3.3. Évaluer les pratiques de protection des données des fournisseurs et des sous-traitants	Annuelle	
	Réaliser des formations pour les employés		
	3.4. Organiser des formations régulières pour maintenir les connaissances des employés sur le RGPD	Annuelle	
	Analyser les incidents de violation de données		
	3.5. Analyser les incidents de violation de données pour déterminer les mesures correctives à prendre	6 mois	
	Améliorer continuellement les mesures de protection des données		
	3.6. Mettre en place des plans d'amélioration continue pour renforcer la protection des données	12 mois	
	Total	12 mois	

V) Annexe 2 : Focus cadre règlementaire RDGP

Le Règlement Général sur la Protection des Données (RGPD) est une réglementation européenne qui vise à renforcer la protection des données personnelles des citoyens européens. Cette réglementation a été mise en place en 2018 et s'applique à toutes les organisations qui traitent des données personnelles, y compris les établissements médico-sociaux.

Le RGPD impose un certain nombre d'obligations aux organisations, telles que l'obligation de mettre en place des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données personnelles, ainsi que l'obligation de garantir le respect des droits des personnes concernées par les données traitées, tels que le droit d'accès, de rectification, d'effacement et d'opposition.

Dans le contexte des établissements médico-sociaux, il est important de noter que le RGPD s'applique à toutes les données personnelles traitées dans le cadre des activités de l'établissement, qu'il s'agisse des données des patients, des bénévoles, des salariés, etc. De plus, les données de santé sont considérées comme des données sensibles et doivent donc faire l'objet d'une protection renforcée.

Enfin, le RGPD prévoit des sanctions financières importantes en cas de non-conformité, qui peuvent atteindre jusqu'à 4% du chiffre d'affaires annuel global de l'organisation. Il est donc essentiel pour les établissements médico-sociaux de se conformer à cette réglementation afin d'assurer la protection des données personnelles et éviter les sanctions financières.

Voici un détail plus complet des principales dispositions du RGPD en matière de protection des données personnelles :

- Champ d'application : Le RGPD s'applique à toutes les organisations, quels que soient leur taille et leur secteur d'activité, qui traitent des données personnelles de personnes résidant dans l'Union européenne.
- Définitions : Le RGPD définit les termes clés tels que "données personnelles", "traitement de données", "responsable du traitement", "sous-traitant", "consentement", "violation de données", etc.
- Principes de traitement : Le RGPD énonce les principes de traitement des données personnelles, à savoir la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la conservation, l'intégrité et la confidentialité.
- Droits des personnes concernées : Le RGPD confère des droits importants aux personnes concernées par les données traitées, tels que le droit d'accès, de rectification, d'effacement, d'opposition, de limitation du traitement et de portabilité des données.
- Obligations des responsables et sous-traitants : Le RGPD impose des obligations aux responsables et aux sous-traitants du traitement des données personnelles, tels que la mise en place de mesures de sécurité techniques et organisationnelles appropriées, la notification des violations de données, la tenue d'un registre des activités de traitement, etc.
- Transferts de données hors de l'UE : Le RGPD impose des conditions strictes pour le transfert de données personnelles en dehors de l'Union européenne.

- Sanctions : Le RGPD prévoit des sanctions financières importantes en cas de non-conformité, pouvant atteindre jusqu'à 4% du chiffre d'affaires annuel global de l'organisation.

Dans le contexte des établissements médico-sociaux, il est important de noter que le RGPD s'applique à toutes les données personnelles traitées dans le cadre des activités de l'établissement, qu'il s'agisse des données des patients, des bénévoles, des salariés, etc. Les données de santé sont considérées comme des données sensibles et doivent donc faire l'objet d'une protection renforcée. Les établissements médico-sociaux doivent donc se conformer à cette réglementation pour garantir la protection des données personnelles et éviter les sanctions financières.

HISTORIQUE DU DOCUMENT

- ⇨ Date de création : 04/05/2023
- ⇨ Validation en CA le
- ⇨ Soumis au CVS le
- ⇨ Présentation en Commission le
- ⇨ Transmis aux Autorités de tarification le
- ⇨ Présentation aux Professionnels le
- ⇨ Présentation aux Personnes accompagnées le

ÉMARGEMENT

	Rédaction	Validation	Approbation
NOM - Prénom			
Fonction			
Date et signature	____/____/_____	____/____/_____	____/____/_____