Apei Les Papillons Blancs Hénin - Carvin	Politique générale de gestion des données à caractère personnel
Processus INFORMATIQUE	APEI-INF-P-03

OBJET :	DOMAINE D'APPLICATION :
Cette procédure décrit les engagements de l'association pris dans le cadre de la démarche RGPD.	Cette procédure s'applique à l'ensemble des établissements et services de l'APEI Hénin Carvin et ses sous-traitants. L'ensemble des professionnels de l'APEI Hénin Carvin avec ses propres traitements ou ceux réalisés par ses sous-traitants.

Diffusion	Directrice Générale Directeur du Développement et de la Qualité Directeurs de Pôle Directeurs Adjoints Chefs de service Secrétariat Directeur des Ressources Humaines Directeur Administratif et Financier Référent RGPD/ Responsable QHSE – Service QHSE DPO

	Nom - Prénom	Fonction	Date	Visa
Rédacteur	HUNET Marlène	Responsable Qualité-GDR	13/01/23	
Vérifié par	MELIET François	DPO	12/1/2023	
	MONSEU Brigitte	Directeur Qualité	16/9/23	
Approuvé par	DELORY Aline	Directrice Générale	16/01/2023	

EVOLUTION DU DOCUMENT

Version	Date	Objet
01	Novembre 2022	Création de la procédure

DOCUMENTS ASSOCIES :

-APEI-INF-P-02 : Procédure en cas de violation de données
-APEI-INF-P-04 : Procédure de droit d'accès
-APEI-INF-P-05 : Procédure de droit d'effacement

Apei Les Papillons Blancs Hénin - Carvin	Politique générale de gestion des données à caractère personnel
Processus INFORMATIQUE	APEI-INF-P-03

SOMMAIRE

Les engagements de l'APEI en matière de protection des données à caractère personnel

Le respect de la vie privée et de la protection des données à caractère personnel constitue un facteur de confiance, valeur à laquelle tient particulièrement l'APEI, en s'attachant au respect des libertés et droits fondamentaux de chacun.

La présente politique de gestion des données à caractère personnel témoigne des engagements mis en œuvre par l'APEI et de l'ensemble de ses collaborateurs dans le cadre de ses activités quotidiennes pour une utilisation responsable des données personnelles.

Cette politique est susceptible d'être mise à jour pour prendre en compte les évolutions législatives et réglementaires, et tout changement dans l'organisation de l'APEI ou dans les offres et services proposés.

Une démarche mutualisée de mise en conformité

Le 25 mai 2018, est entré en vigueur le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 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 (Règlement Général sur la Protection des Données dit « RGPD »).

A cette occasion, **huit associations du Pas-de-Calais** (Apei de Béthune, Apei du Boulonnais, Afapei du Calaisis, Apei d'Hénin/Carvin, Apei de Lens, Apei de Saint Omer, le GAM et l'Udapei 62) **et une association de l'Oise** (Unapei 60) ont engagé de manière commune une démarche de mise en conformité aux nouvelles exigences réglementaires posées par le RGPD.

Par l'adoption de la présente politique, les associations engagées dans cette démarche souhaitent réaffirmer leur appartenance à ce groupe de travail mutualisé, ainsi que l'objectif initialement défini de parvenir à un degré de maturité commun.

La protection des données personnelles : une composante essentielle de la démarche qualité-gestion des risques

Depuis la loi du 2 janvier 2002 rénovant l'action sociale et médico-sociale, les ESSMS ont l'obligation de procéder à une évaluation régulière de leurs activités et de la qualité des prestations délivrées aux personnes accueillies.

Le 8 mars 2022, la Haute Autorité de Santé, chargée d'élaborer la procédure d'évaluation nationale en la matière, a intégré à cette dernière deux critères liés au respect des dispositions du RGPD :

- Désormais, les ESSMS doivent en premier lieu garantir la confidentialité et la protection des informations et données relatives à la personne accompagnée ;
- Les ESSMS doivent par ailleurs veiller au respect, par leurs professionnels, des règles de sécurisation des données, des dossiers et des accès.

Gouvernance de la protection des données personnelles

- **Le Délégué à la Protection des Données (DPD) / Data Protection Officer (DPO)**

Afin de préserver la vie privée et la protection des données à caractère personnel de tous, les APEI ont désigné un Délégué à la Protection des Données (DPD)/Data Protection Officer (DPO) dont les services sont mutualisés entre les neuf associations.

Le DPO est un gage de confiance, spécialisé dans la protection des données personnelles. Il est chargé de veiller à la préservation de la vie privée et à la bonne application des règles de protection des données personnelles. Il est l'interlocuteur privilégié de la Commission Nationale de l'Informatique et des Libertés (CNIL), et de toute personne concernée par une collecte ou un traitement de données à caractère personnel.

Le choix a été fait de désigner un DPO externalisé, disposant des compétences spécialisées et du niveau d'expertise requis pour mener à bien cette mission. Ce choix garantit également l'absence de conflit d'intérêts, notamment à l'occasion des phases d'audits et de contrôles de la démarche.

- **Les référents RGPD associatifs**

En parallèle, les associations nomment un référent RGPD au sein de leur propre organisation, identifié comme l'interlocuteur clé du DPO au sein de chaque association. Le référent RGPD assure la centralisation des demandes internes à chaque association. Il est garant de la compréhension par le DPO de l'organisation interne de son association et un relais auprès des autres acteurs susceptibles d'être mobilisés (DRH, DSI, Directeurs d'établissements...). Il peut également être le bénéficiaire des formations et sensibilisations du DPO avant d'assurer lui-même la formation au sein de son association.

- **Le bilan du DPO**

Ce bilan est établi annuellement par le Délégué à la Protection des Données des neuf associations engagées dans la démarche de conformité au RGPD et constitue un élément essentiel de la démarche de mise en conformité au RGPD : il permet à l'association d'assurer la traçabilité des actions menées sur l'année écoulée et d'en assurer le reporting aux équipes de Direction.

Ce bilan est par ailleurs tenu à la disposition de la CNIL qui demande à l'organisme de constituer et regrouper la documentation permettant de démontrer le respect des obligations prévues par le règlement européen.

- **Les comités de pilotage des référents RGPD**

Composé des référents RGPD des neuf associations engagées dans la démarche de conformité RGPD, le comité des référents se réunit chaque trimestre en présence du DPO.

Ce comité est l'occasion de faciliter l'échange entre les référents et le DPO des associations, de remonter des questions communes, d'apprécier la mesure dans laquelle les différents axes d'amélioration sont mutualisables et de valider certains choix stratégiques.

- Le comité de pilotage interne

Composé de l'équipe de Direction des établissements et du siège social de l'association, le comité de pilotage interne se réunit a minima deux fois par an en CODIR.

L'objectif est de déployer la feuille de route inter-APEI en plan d'action à l'échelle de l'association. En parallèle, le Directeur de la qualité et le référent RGPD assurent le lien avec le DPO.

Campagne annuelle de contrôle

Chaque année, les neuf associations engagées réalisent par leurs propres moyens ou font réaliser par un prestataire désigné de manière commune des opérations d'audit et de contrôle portant sur la sécurité des données personnelles qu'elles traitent.

Ces opérations d'audit et de contrôle se déclinent comme suit :

- **Evaluation du niveau de maturité RGPD**

L'ensemble des associations s'engagent à réévaluer leur niveau de maturité au RGPD en prenant appui sur le référentiel suivant : ***Guide CNIL « Autoévaluation de maturité en gestion de la protection des données »***, publié en septembre 2021.

Pour consolider cette autoévaluation, les associations prennent aux termes de la présente politique l'engagement de faire réaliser, de manière annuelle, l'une des opérations de contrôle suivantes :

- Audit de conformité à la réglementation sur la protection des données personnelles
- Campagne d'audits flash
- Contrôle « à blanc » du respect des droits des personnes

- Contrôle aléatoire du contenu des zones de commentaires libres / Contrôle aléatoire des habilitations
- Contrôle de la conformité du site web de l'association

Les comptes-rendus des ces opérations d'audits et de contrôle ainsi que le diagnostic d'autoévaluation associé seront intégrés au bilan annuel d'activité élaboré par le DPO à chaque fin d'année civile.

- **Réalisation d'audits de sécurité informatique**

L'ensemble des associations prennent par ailleurs l'engagement de faire tester, analyser et évaluer l'efficacité des mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité informatique des traitements.

Pour ce faire, les associations prennent aux termes de la présente politique l'engagement de faire réaliser, de manière annuelle, l'un des diagnostics techniques suivants :

- Audit complet de sécurité du SI
- Audit d'infrastructure
- Rédaction de spécifications informatiques conformes RGPD (purge, archivage, anonymisation)
- Tentative d'intrusion physique sur site
- Campagne de « phishing » (ou « hameçonnage »)
- Test d'intrusion (« pen tests ») de sites web ou de logiciels exposés sur le web

Formation / Sensibilisation des professionnels

Les associations se sont fixées pour objectif de mener leurs professionnels à un niveau de connaissance commun en matière de protection des données personnelles, mais également de leur communiquer les bonnes pratiques en matière de gestion des données personnelles ainsi que les règles qu'elles s'efforcent de définir au fur et à mesure de leur démarche de conformité au RGPD.

Plusieurs vecteurs de formation / sensibilisation des professionnels sont exploités, parmi lesquels :

- Le déploiement d'un **plan de formation / de sensibilisation** des professionnels acteurs du dispositif de conformité.
  Ce plan tient compte du degré d'exposition des professionnels aux enjeux liés à la protection des données personnelles : ainsi, les opérationnels les plus exposés assistent à des ateliers de sensibilisation en présentiel et sont invités à prendre connaissance d'infographies ou de procédures portant sur des thèmes spécifiques de la protection des données, tandis que pour les opérationnels moins exposés, la diffusion de courtes vidéos de sensibilisation et la réalisation d'une sensibilisation e-learning est peu à peu déployée ;

- L'insertion d'une **clause de confidentialité** dans le contrat - quelle qu'en soit la forme - passé avec toute personne amenée à exercer une fonction au sein de l'association (salarié, stagiaire, alternant, bénévole, intervenant ponctuel...).
  Cette clause s'ajoute à l'obligation de loyauté, et par conséquent de discrétion, à laquelle est tenu le professionnel au titre des dispositions du Code de travail.
  Elle s'ajoute plus spécifiquement, dans le secteur médicosocial et pour les professionnels concernés, au respect du secret professionnel dont la violation est réprimée par le Code pénal ;

- La diffusion d'une **charte informatique**, à jour de la réglementation sur la protection des données personnelles et rendue opposable aux salariés après consultation des instances représentatives du personnel.
  Cette charte a pour but de traduire de manière concrète les engagements des salariés en matière d'utilisation des outils et ressources informatiques mis à disposition de ces derniers par l'association.

Feuille de route de la démarche RGPD

Au-delà des lignes directrices de la démarche RGPD ci-dessus édictées et de la description organisationnelle livrée par les associations au sein de la présente politique, ces dernières portent à l'attention des personnes concernées avoir défini ensemble une feuille de route qui se matérialise par la réalisation d'un certain nombre d'actions, au nombre desquelles :

- La création et la tenue à jour d'un registre des traitements par association – *article 30 du RGPD*
- La rédaction, dans un format adapté au public concerné, et la diffusion de mentions d'information et de recueil du consentement des personnes concernées – *articles 12 à 14 du RGPD*
- L'élaboration et la diffusion de procédures de traitement des droits « Informatique et Libertés » des personnes – *articles 15 à 23 du RGPD*
- L'élaboration et la diffusion d'une procédure de gestion des violations de données – *articles 33 & 34 du RGPD*
- La réalisation d'analyses d'impact sur la protection des données personnelles (AIPD) pour tout traitement présentant des risques particulièrement élevés pour la vie privée des personnes – *article 35 du RGPD*
- L'encadrement des relations contractuelles avec ses prestataires et partenaires « sous-traitants » au sens de la réglementation – *article 28 du RGPD*

Confidentialité & sécurité des données personnelles

L'APEI assure mettre en œuvre des mesures de protection des systèmes d'information adaptées à la nature des données qu'elle traite dans le cadre de ses activités.

Absence de transferts hors UE

Il est ici précisé que l'APEI ne procède à aucun transfert de données personnelles en dehors de l'Union Européenne.

Les droits des personnes

Les personnes concernées disposent de différents droits sur leurs données personnelles, à savoir :

- Le droit d'accéder ou de demander copie des données personnelles qui les concernent – *article 15 du RGPD*
- Le droit de demander l'effacement des données personnelles qui les concernent – *article 17 du RGPD*
- Le droit de faire rectifier leurs données personnelles lorsqu'elles sont inexactes et/ou de faire compléter leurs données personnelles lorsqu'elles sont incomplètes – *article 16 du RGPD*
- Le droit de demander la limitation du traitement des données personnelles qui les concernent – *article 18 du RGPD*
- Le droit à la portabilité de leurs données personnelles – *article 20 du RGPD*
- Le droit de s'opposer au traitement de leurs données personnelles pour des raisons tenant à leur situation particulière, sauf si des motifs légitimes et impérieux pour le traitement prévalent sur leurs intérêts et sur leurs droits et libertés – *article 21 du RGPD*
- Le droit de définir des directives relatives au traitement des données personnelles après leur décès – *article 85 de la loi relative à l'informatique, aux fichiers et aux libertés*

L'association s'engage à respecter l'ensemble de ces droits. Elle s'est à cette fin dotée de procédures de traitement des droits « Informatique et Libertés » des personnes dont elle a assuré la diffusion auprès de destinataires ciblés et dont elle vérifie régulièrement la bonne application.
Aux termes de cette procédure, l'association a prévu que tout droit listé ci-dessus et exercé conformément à la réglementation sur la protection des données personnelles peut être exercé auprès du Délégué à la protection des données, soit par courrier électronique à l'adresse suivante : dpo@apei-henin.com, soit par courrier postal à l'adresse suivante : « APEI Hénin/Carvin – A l'attention du DPO – Boulevard Jean Moulin – 62 110 Hénin-Beaumont ».
L'association prend l'engagement de donner suite à toute demande dans un délai raisonnable et, en tout état de cause, dans les délais fixés par la réglementation.