LARNAY Sagesse

ACCUEIL DE PERSONNES EN SITUATION DE HANDICAPS SENSORIELS

POLITIQUE DU SYSTEME DE MANAGEMENT DES DONNEES A CARACTERES PERSONNELLES

F.A.M
Foyer d'Accueil Médicalisé

F.V
Foyer de Vie

E.H.P.H.S.A.D
Etablissement d' Hébergement pour Personnes Handicapées Sensorielles, Agées Dépendantes

SMDCP

Nom du responsable du traitement : Olivier Besseron

Nom du COORDINATEUR : Bertrand Blondeau

Date de mise en vigueur : 01/01/2020

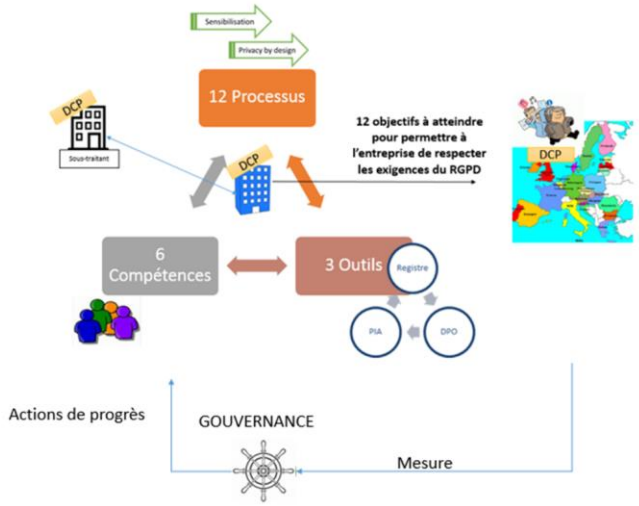
Date de mise à jour

Date	Auteur	Modification
01/01/2020	B.BLONDEAU	Validation document
08/12/2022	B.BLONDEAU	Responsable + comité

Commenté [BB1]: Ce document permet de présenter le fonctionnement du comité de pilotage, les procédures mises en place…

Table des matières

La présente politique décrit les mesures techniques et organisationnelles qui permettre à l'association Larnay Sagesse de respecter dans le temps les exigences du RGPD et de pouvoir le démontrer.



1. RESPONSABILITE

1.1. Objectifs

Le responsable du traitement doit fournir la preuve de son implication dans l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration du SMDCP.

1.2. Composition du comité « Informatique et libertés »

La gouvernance du SMDCP est assuré par un comité intitulé « Informatique et libertés ». Il est composé de :

- Mr Besseron, directeur général, et agissant en tant que responsable des activités traitement
- Mr Blondeau, agissant en tant que coordinateur et animateur du comité
- Mme Morteau et Mme Mouzaoui, assistantes direction des établissements
- Mme Brousse, Responsable RH
- Mr Bonin, Responsable Qualité-développement

Commenté [BB2]: Mise à jour comité

1.3. Responsabilités du comité

Le présent comité fournit les ressources nécessaires à la mise en œuvre, au fonctionnement et au cycle de vie du SMDCP.
Il s'assure que la présente politique est appliquée.

1.4. Fréquence des comités

Le comité se réunit 1 fois par an.

1.5. Déclaration du Coordinateur

Mr Blondeau a été désigné coordinateur de la gestion des DP au sein de l'association.

1.6. Responsabilité du comité

- Piloter les plans de progrès
- Sensibiliser les employés impliqués dans le traitement des DCP

1.7. Responsabilité du COORDINATEUR

Les responsabilités de Mr Blondeau sont les suivantes :

- Animer le comité « Informatique et libertés »
- Tenir à jour le registre des traitements
- Contrôler le respect du règlement et ses évolutions
- Informer et conseiller le responsable de traitement et les sous-traitants
- Conseiller sur la réalisation des analyses d'impact et en vérifier l'exécution
- Coopérer avec la CNIL
- Préparer et rédiger le bilan annuel

1.8. Revue des traitements

Le registre des traitements est revu une fois par an ou lorsqu'un évènement le nécessite.

1.9. Revue du système de management

Le SMDCP est revu une fois par an ou lorsqu'un évènement le nécessite.

1.10. Validation du bilan annuel

Monsieur Blondeau, instruit le bilan qui est partagé par le comité.
Après discussion le bilan est amendé et validé.

2. TRAITEMENTS

2.1. Objectifs

Disposer d'un registre des activités de traitement à jour.

S'assurer que les mesures de conformité des traitements de DCP sont effectivement prises en compte en cas de traitements nouveaux ou modifiés.

2.2. Tenue du registre des traitements

L'ensemble du personnel est informé de ses obligations à signaler tout traitement, tout nouveau traitement ou tout traitement ultérieur de DCP à Mr BLONDEAU

3. GESTION DES DROITS DE LA PERSONNE CONCERNEE

3.1. Objectifs

Faire en sorte que les personnes concernées aient la capacité d'exercer effectivement leurs droits en matière de protection de la vie privée.

S'assurer que les formules de demande de consentement sont alignées sur la finalité du traitement.

3.2. Politique de protection des données

Le document de politique générale de protection des données, précise les engagements de l'association en matière de gestion des données à caractère personnel : Finalité de la collecte, consentement, conservation, informations aux personnes concernées, demandes de la personne concernée.

3.3. Procédures associées à la gestion des droits

Les procédures suivantes sont documentées et testées :

- Demande d'effacement
- Demande de consultation de ses données
- Demande de portabilité

Toutes les demandes sont archivées.

3.4. Point de contact unique

Toute personne concernée souhaitant exercer ses droits d'accès à ses données, peut envoyer sa demande par mail à RGPD@larnay-sagesse.fr.

4. GESTION DE LA SOUS TRAITANCE DCP

4.1. Objectifs

S'assurer que les responsabilités en matière de conformité des traitements de DCP sont correctement identifiées, réparties et prises en comptes par les sous-traitants.

4.2. Politique en matière de recours à la sous-traitance

Le COORDINATEUR est impliqué dans le processus de choix d'un nouveau sous-traitant.

4.3. Liste des sous-traitants DCP

Le COORDINATEUR tient à jour la liste des sous-traitants.

- *Liste stockée dans la boite à outils, sous : RGPD*

Commenté [BB3]: Mise à jour du lien

4.4. Contrôle des Sous-Traitants

Les contrats de sous-traitance sont vérifiés à chaque date anniversaire pour voir s'ils portent les mentions nécessaires en matière de conformité des traitements de DCP.

De plus le sous-traitant doit être engagé dans une démarche RGPD qui doit être formalisé dans le contrat de sous-traitance.
Dans le cas où il est amené à être en possession des données personnelles de résidents et/ou professionnels, il doit nous communiquer :

- Nom des intervenants qui auront accès à ces données
- Information sur le lieu de stockage et le temps de conservation des données
- Attestation de destruction des données

5. SECURITE A LA CONCEPTION (Privacy by design)

5.1. Objectifs

Lors de changement d'outils traitant des données personnelles ou de leurs mises à jour, il sera vérifié qu'ils respectent les exigences en matière de sécurité, voir Politique de sécurité du système d'information.

5.2. Implication du COORDINATEUR

Avis consultatifs sur le choix de la solution

5.3. Ressources

Le coordinateur aura accès aux documents techniques et de politique de gestion des données du prestataire.

5.4. Facteurs déclenchant l'exécution d'une évaluation des risques

Traitement de données sensibles ou/et médicales.

6. SECURITE PAR DEFAUT (Privacy by default)

6.1. Objectifs

En relation avec le responsable informatique de l'association, mettre en œuvre les mesures de protection sélectionnées afin de répondre aux objectifs de disponibilité, d'intégrité et de confidentialité des DCP.

6.2. Référent sécurité

Responsable IT

6.3. Politique de sécurité

Pour les logiciels qui traitent des données personnelles :

- Gestion des accès par mot de passe ou par annuaire LDAP
- Mots de passes complexes 10 caractères minimum
- Accès nominatifs
- Gestion des habilitations
- Communications chiffrées (interne ou externe)
- Mot de passe chiffrer dans la base SQL
- Journalisation des accès
- Extraction de données selon demandes légales

Commenté [BB4]: De 8 à 10 caractères

7. ANALYSE D'IMPACT (Privacy Impact Assesment)

7.1. Objectifs

Être en capacité de réaliser un PIA lorsque le SMDCP l'exige (données sensibles ou/et médicales).

7.2. Méthode d'analyse de risque

Définition de scénarios possibles avec leur valeur d'occurrence = Niveau de vraisemblance
4 niveaux de gravite en fonction leur impact potentiel dans 4 domaines
Domaines :

- Impact vie privée
- Juridique
- Réputation
- Perte financière

Gravité :

Critères de gravité					
	Autorité	Conséquences			
	RGPD	Impacts sur la vie privée	Réputation	Juridique	Perte financière
Critique	Na	Non applicable	Perte de confiance irréversible suite à une campagne hostile (médias, réseaux...)	Tribunal pénal avec amende significative et peine de prison	4 fois le BFR
Très Important	Non-conformité majeure	Affection matériel, physique ou psychologique grave et irréversible	Perte de crédibilité temporaire vis-à-vis de clients ou de partenaires.	Tribunal pénal avec amende significative ou Injonction à cesser une activité	2 fois le BFR 2 à 4% du CA
Important	Non-conformité mineure	Affection matériel, physique ou psychologique mineure et passagère	Plainte formalisée avec avertissement rendu public	Tribunal civil avec sanctions pécunières	Quelques milliers d'euros
Négligable	Remarque	Désagrément surmontable	Rumeur	Mise en demeure avec action en réparation	Quelques euros

Le niveau de risque est calculé de la façon suivante :

*Niveau de vraisemblance * Niveau de gravité = Niveau de risque*

7.3. Contenu standard d'un rapport PIA

Voir annexe : PIA.pdf

8. SENSIBILISATION, FORMATION

8.1. Objectifs

S'assurer que le personnel à qui a été affecté les responsabilités définies dans le SM DCP, a les compétences nécessaires pour exécuter les tâches requises.

S'assurer que tout le personnel approprié a conscience de la pertinence et de l'importance de ses activités liées aux traitements des DCP.

8.2. Programme de sensibilisation

½ journée de sensibilisation aux personnels concernées.

8.3. Campagne de communication

Campagne sur l'intranet de l'association pour sensibiliser tout le personnel à la problématique des DCP.
Présentation du SMDCP pendant une réunion institutionnelle.

9. RELATION AVEC LA CNIL

9.1. Objectifs

Etre organisé pour répondre à des sollicitations ou à des poursuites.
Etre organisé pour informer la CNIL d'une violation de nos DP.

9.2. Processus de réponse

Dans le cas d'une sollicitation de la CNIL :

- Informer le responsable de traitement
- Informer le Coordinateur

Dans le cas d'une violation de nos DP :

- Informer le prestataire pour analyse de l'incident
- Recenser les DP concernées
- Déclarer a la CNIL sous 48H
- Porter plaintes auprès de la gendarmerie
- Informer les personnes concernées par la violation des données

10. EVALUATION, AUDIT, AMELIORATION

10.1. Objectifs

Vérifier le SMDCP est mis en œuvre conformément aux politiques définies.

10.2. Programme d'audit ou d'évaluation

Tous les 2 ans, le SMDCP doit être audité dans son ensemble.

11. Gestion de la documentation et les preuves

11.1. Objectifs

Etablir et conserver des enregistrements pour apporter la preuve que l'association est organisée pour respecter les exigences du RGPD

Disposer d'une documentation : procédures, modèles de courrier et mentions légales.

11.2. Liste des documents de références

Les documents ci-dessous sont stockés sous :

- Dossier « boite à outils » : RGPD
- GED dossier RGPD

Commenté [BB5]: Mise à jour des liens

Nom du document
Système de mangement des DCP
Politique de protection des données Résidents
Politique de protection des données Salariés
Politique de sécurité
Registre des traitements
Signalement d'un nouveau traitement auprès du Coordinateur
Procédure de gestion des demandes concernant les DCP
Courrier de réponses CAS professionnel
Courrier de réponses CAS résident
Formulaire de demande de consultation de DP
Procédures informatique

11.3. Accessibilité des documents de politique

Les documents concernant la politique de gestion des données personnelles sont gérés par le COORDINATEUR et accessibles sur le site internet pour l'ensemble du personnel et les représentants légaux des résidents.

Commenté [BB6]: A voir si nécessaire

11.4. Documents à valeur de preuve

Les documents concernant les demandes et réponses seront classés dans la GED où un horodateur certifié permet de rendre compte de la date d'enregistrement.

12. Gestion des opérations du SMDCP

12.1. Objectifs

Disposer d'indicateurs pour piloter l'efficacité des processus du SMDCP.

Rédiger le bilan annuel.

12.2. Planification des activités

Les réunions du comité de pilotage donneront les objectifs à atteindre au cours de l'année avec les ressources nécessaires au coordinateur.

12.3. Tableau de bord

Voir annexe

12.4. Production du bilan annuel

Un bilan sera rédigé par le COORDINATEUR présenté au comité lors de la réunion annuelle et validée.