CENTRE DE RÉHABILITATION
château de colpach

POLITIQUE GENERALE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Validée par le Conseil d'administration de la Fondation Emile Mayrisch Croix-Rouge a.s.b.l. le 18 septembre 2019.

Audience : Cette politique s'applique à toute personne physique agissant au service de la Fondation Emile Mayrisch Croix-Rouge a.s.b.l. et du Centre de Réhabilitation du Château de Colpach.

Point de contact : Data Protection Officer, Fondation Emile Mayrisch Croix-Rouge a.s.b.l.

Table des matières

PREAMBULE

Attachés au respect de la vie privée et à la protection des données à caractère personnel qui leurs sont confiées dans le cadre de l'exécution de leurs missions, le Centre de Réhabilitation du Château de Colpach (ci-après dénommé « CRCC »), établissement hospitalier spécialisé et la Fondation Emile Mayrisch Croix-Rouge a.s.b.l (ci-après dénommée « FEM ») en sa qualité d'organisme gestionnaire du CRCC, s'engagent à respecter la législation applicable en matière de protection des données à caractère personnel, en particulier le Règlement Général sur la Protection des Données à caractère personnel 679/2016 du 27 avril 2016 (dit « GDPR » ou « RGPD ») ainsi que les lois luxembourgeoises du 1er août 2018 sur la protection des données à caractère personnel.

Pour les besoins de clarté du présent document, seule la FEM sera évoquée dans la suite du document, étant entendu que le CRCC fait partie intégrante de la FEM.

La présente politique de protection des données à caractère personnel (ci-après dénommée « Politique ») formalise les engagements de la FEM pour une utilisation responsable des données à caractère personnel dans le cadre de l'exécution de ses activités au quotidien. Cette politique a pour objectifs de :

- Permettre à la FEM de se mettre et de rester en conformité avec les obligations légales applicables en matière de protection des données,

- décrire les rôles et responsabilités en matière de gestion et de protection des données personnelles,

- formaliser les principes que la FEM entend mettre en application pour assurer la protection des données à caractère personnel.

La présente Politique n'a pas pour but de constituer un frein aux activités quotidiennes réalisées par les collaborateurs de la FEM dans le cadre de l'exécution de leurs missions, mais de les aider à remplir ces missions dans le respect de la loi.

1. DOMAINE D'APPLICATION DE LA POLITIQUE

La présente Politique s'applique à tous les traitements de données à caractère personnel, automatisés ou non (donc y inclus les dossiers papiers) mis en œuvre la FEM dans le cadre de ses activités.

Elle s'applique à l'ensemble des collaborateurs de la FEM lorsqu'ils interviennent directement ou indirectement dans des activités incluant le traitement de données à caractère personnel ou la gestion des systèmes d'information.

2. DEFINITIONS

Dans la Politique, les termes suivants prennent les sens qui suivent:

- **CNPD** : Commission Nationale pour la Protection des Données : autorité indépendante de contrôle en matière de protection des données personnelles compétente pour les traitements mis en œuvre par la FEM ;

- **Collaborateur de la FEM** : toute personne physique agissant au service de la FEM (personnel interne ou externe, bénévoles, stagiaires, apprentis, etc.) ;

- **Données à caractère personnel, Données personnelles** ou **données** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée personne concernée) ;

- **DPO** : *Data Protection Officer* ou délégué à la protection des données, au sens de l'article 37 du RGPD ;

- **FEM** : désigne la Fondation Emile Mayrisch Croix-Rouge a.s.b.l, en ce compris le Centre de Réhabilitation du Château de Colpach ;

- **Personne physique identifiable** : toute personne physique pouvant être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

- **Sous-traitant**: la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

- **Traitement**: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés

- **Responsable du traitement** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens de traitement de données à caractère personnel ;

- **Violation de données à caractère personnel**: toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

3. ROLE DE LA FEM PAR RAPPORT AUX TRAITEMENTS DES DONNEES A CARACTERE PERSONNEL

La FEM est responsable de la mise en conformité et du maintien de la conformité aux obligations légales qui lui sont directement applicables.

La FEM agit comme responsable des traitements des Données à caractère personnel dans le cadre de l'exécution de ses missions et comme sous-traitant d'autres entités ou partenaires tiers pour tous les traitements qu'elle réalise exclusivement pour leur compte et sur leurs instructions.

4. PRINCIPES APPLICABLES A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

La FEM s'assure que tout Traitement de Données à caractère personnel qu'elle met en œuvre respecte les principes relatifs à la protection de données.

4.1) Licéité, loyauté et transparence

La FEM ne traite des Données à caractère personnel que lorsque ce Traitement est basé sur au moins un des fondements juridiques énumérés par le règlement (contrat, mission d'intérêt public, consentement, obligation légale, intérêts vitaux de la personne, intérêt légitime).

En outre, conformément au principe de transparence et de loyauté, la FEM s'engage à informer les personnes concernées par le biais de moyens et supports adaptés.

4.2) Minimisation des données

La FEM minimise la collecte des données personnelles. Seules les Données à caractère personnel strictement nécessaires pour atteindre les finalités poursuivies sont collectées.

4.3) Limitation des finalités

Les finalités des traitements mis en œuvre par la FEM sont explicites et légitimes. De plus, les données personnelles ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités.

4.4) Exactitude des données

La FEM s'engage à mettre à jour les Données à caractère personnel afin d'en garantir l'exactitude. A cet effet, elle s'engage à rectifier les données lorsque celles-ci sont inexactes ou incomplètes.

4.5) Limitation de conservation

Les durées de conservation des données personnelles sont portées à la connaissance des personnes concernées, et varient selon la nature des données, la finalité des traitements, ou les exigences légales ou réglementaires. Au-delà de ces durées de conservation, les Données à caractère personnel doivent être supprimées, anonymisées, ou archivées.

4.6) Intégrité et confidentialité des données

La nature des missions de la FEM la conduit à traiter pour une part essentielle de ses activités, des données sensibles concernant des personnes vulnérables. Conscient de ce que la survenance des risques liés au Traitement des Données à caractère personnel peut entrainer un impact important pour les personnes concernées et aussi pour l'établissement et ainsi entraver ses missions, des mesures de sécurité physiques, logiques et organisationnelles appropriées sont prévues pour garantir la sécurité et confidentialité des données traitées.

En outre, la FEM s'engage à renforcer la culture de la sécurité de l'information et de la protection des données au sein de tous ses services au moyen de la sensibilisation de l'ensemble de ses collaborateurs.

En cas de recours à la sous-traitance, la FEM ne collabore qu'avec des Sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences de protection des données personnelles et qui s'engagent à respecter les dispositions légales et règlementaires applicables en matière de protection des données.

Les Données à caractère personnel peuvent faire l'objet de transferts vers des pays situés hors de l'Union Européenne. Si tel est le cas, les personnes concernées en sont précisément informées, et des mesures spécifiques sont prises pour encadrer ces transferts.

4.7) Responsabilité (Accountability)

Registre de traitement

La FEM doit tenir à jour les registres de tous les traitements de Données à caractère personnel mis en œuvre contenant à minima les informations légales imposées par la législation en vigueur.

Pour chaque nouveau Traitement, le DPO complète le registre avec l'assistance du responsable du service concerné par ce Traitement.

Le DPO s'assure de la mise à disposition du registre :
- à la CNPD, dans les cas prévus par la loi,
- au Conseil d'Administration et au Comité de Direction sur demande,
- aux responsables de services, pour les traitements qui les concernent.

Violation de Données personnelles

En cas de Violation de Données personnelles, le Comité de Direction, le DPO et chaque collaborateur de la FEM concerné doivent agir selon les prescriptions de la procédure afférente.

Gestion des droits des personnes concernées

La FEM est tenue de, et s'engage à respecter les droits des personnes concernées qui leur sont conférés par la loi. Sous réserve des dispositions légales et réglementaires en

vigueur, la FEM met en œuvre tous les moyens pour que les personnes concernées soient informées du Traitement de leurs Données à caractère personnel, des droits dont elles disposent et des moyens d'exercer ces droits.

La FEM s'engage par ailleurs à répondre aux demandes d'exercice des droits émanant des personnes concernées dans les délais légaux.

Gestion des risques

Conformément à l'approche par les risques préconisée par le RGPD, la FEM s'engage à prendre en compte, les exigences de protection des Données à caractère personnel dès les phases de planification de tout nouveau projet de Traitement de données ou de modification d'un Traitement de données existant, afin d'identifier les risques en amont, de réaliser des analyses d'impact sur la protection des données dans les cas où cela est requis et de prendre les toutes mesures adéquates de protection de données dès la conception et par défaut.

Plans de contrôles

Des plans de contrôles internes de conformité des opérations de traitement et de sécurité des supports de traitement des données seront mis en place en fonction des risques identifiés dans une logique d'amélioration continue. En outre, les risques identifiés seront réexaminés périodiquement afin de permettre une mise à jour des différents documents de gouvernance et du plan de mise en conformité.

5. ROLES ET RESPONSABILITES

5.1) Conseil d'Administration

Le Conseil d'Administration de la FEM est responsable de la conformité de l'ensemble des activités de Traitement de données à caractère personnel mis en œuvre par la FEM.

A cet effet, le Conseil d'Administration approuve et soutient la mise en application de la présente Politique.

5.2) Comité de Direction

Le Comité de Direction

- veille à ce que les fonctions et départements concernés par les traitements de Données à caractère personnel associent le DPO en temps utile et lui fournissent les informations nécessaires à l'exercice de ses fonctions;

- veille à ce que le DPO dispose des moyens nécessaires à l'accomplissement de ses missions en toute indépendance, et en particulier que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ;

- veille, dans l'hypothèse où le DPO accomplirait d'autres tâches et missions que

celles dévolues au DPO par la politique, à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts ;

- s'assure que tous ses collaborateurs/trices aient une connaissance suffisante des enjeux de la protection des Données à caractère personnel, par le biais d'opérations de communications, de sessions de sensibilisation et de formations appropriées ;

- s'assure que les fournisseurs et sous-traitants de la FEM interviennent sur les traitements de Données personnelles en vertu d'un cadre contractuel approprié et conforme aux exigences légales.

5.3) DPO

Conformément aux exigences du RGPD, la FEM a nommé un DPO.

Le DPO :

- fait directement rapport au Comité de Direction du CRCC;

- est soumis au secret professionnel ;

- est l'interlocuteur principal de la CNPD et des personnes concernées en cas de litiges ou d'incidents liés à la protection des Données à caractère personnel ;

- informe et conseille la direction ainsi que les collaborateurs de la FEM sur leurs obligations relatives à la protection des Données à caractère personnel ;

- dispense des conseils, sur demande, aux Responsables de traitement lors de la réalisation d'analyse d'impact relative à la protection des Données à caractère personnel et vérifie l'exécution de celle-ci ;

- tient à jour les registres des activités de Traitement de la FEM;

- contrôle le respect de la présente Politique, des documents qui en découlent et de la législation en matière de protection des données personnelles (en particulier le RGPD) ;

- rédige (ou coordonne la rédaction) et s'assure de la mise en place et du respect de procédures et documents déclinant de la Politique pour toutes les activités de la FEM impliquant le Traitement de données personnelles ;

- tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de Traitement compte tenu de la nature, de la portée, du contexte et des finalités du Traitement ;

- Dispense des formations spécifiques et adaptées au niveau d'implication des collaborateurs dans le Traitement des données personnelles et sensibilise l'ensemble des collaborateurs/trices des enjeux de la protection des Données à

caractère personnel, par le biais d'opérations de communications.

5.4) Responsable du service informatique/Responsable de la Sécurité des Systèmes d'information (RSSI)

De manière non exhaustive, il revient au responsable du service informatique et au RSSI de :

- définir et de s'assurer de la mise en œuvre de mesures de sécurité techniques et organisationnelles de nature à assurer la protection des données personnelles contre les risques liés à l'usage des systèmes d'information ;
- collaborer avec le DPO et son équipe en cas de Violation de Données à caractère personnel ;
- concevoir du/des plan(s) d'actions visant à gérer les risques liés à la sécurité de l'information.

5.5) Collaborateurs de la FEM

Il incombe à chaque collaborateur de la FEM de :

- prendre connaissance de la présente Politique, la respecter et la faire respecter ainsi que tous les procédures relatives à la protection des données dans le cadre des traitements qu'ils sont amenés à mettre en œuvre dans le cadre de leurs missions ;
- traiter les Données à caractère personnel dans le strict respect de la vie privée des personnes concernées et en respectant les obligations de secret professionnelle ;
- rapporter au DPO tout incident ou violation de Données à caractère personnel,
- consulter le DPO avant la mise en œuvre de tout nouveau Traitement de Données personnelles.

5.6) Responsables de traitements tiers

Dans les cas où la FEM agit comme Sous-traitant de partenaires tiers, ces derniers sont juridiquement responsables de leurs traitements de Données personnelles.

Néanmoins, certaines obligations incombent à la FEM en qualité de Sous-traitant. la FEM doit :

- disposer d'un cadre contractuel écrit conforme aux exigences du RGPD ;
- tenir un registre de toutes les catégories d'activités de Traitement effectuées pour le compte de tiers. Il incombe du DPO de tenir ce registre à jour.

5.7) Sous-traitants, fournisseurs et partenaires

Lorsque la FEM sous-traite des actes de Traitement de Données personnelles à des partenaires/fournisseurs tiers, la FEM reste juridiquement responsable de ces actes de traitement.

Le DPO veillera à s'assurer, via la réalisation d'analyses de risques, d'audits ou de revues, de la mise en conformité et du respect des exigences du RGPD pour chaque Sous-traitant de la FEM.

6. CONTROLE DE L'APPLICATION DE LA POLITIQUE

Le DPO établit périodiquement un programme d'audits de conformité au RGPD et le soumet pour validation au Comité de Direction.

Ils portent notamment sur :
- le contrôle de la conformité aux exigences légales et à la Politique ;
- le contrôle de l'efficacité des procédures, directives et dispositifs de protection mis en œuvre pour assurer la protection des Données à caractère personnel.

Les résultats des audits sont transmis au Comité de direction, qui prendra les décisions qui s'imposent en fonction de la gravité des points de non-conformité constatés.

7. EVOLUTION DE LA POLITIQUE

La FEM s'engage à faire évoluer la présente Politique afin de prendre en compte les évolutions légales et réglementaires ou technologiques, ainsi que les contraintes opérationnelles des services.

Le DPO assure la veille légale et jurisprudentielle en matière de protection des Données personnelles.

Toute évolution identifiée dans le cadre des activités de veille doit faire l'objet d'une évaluation de son impact sur la Politique. Il incombe au DPO de proposer les ajustements nécessaires pour prendre en compte des évolutions en vue de la validation par le Conseil d'Administration.