RGPD

Sécurité informatique et sécurité de l'information

Politique de l'institution quant à la sécurité des données personnelles

_____

L'institution collecte et traite des données personnelles dans les domaines suivants :

- Bénéficiaires SAAF :

La finalité du traitement est de garantir l'accompagnement optimal de l'enfant dans son projet individualisé.

Les données récoltées sont classifiées comme suit :
- Données administratives nécessaires à la prise en charge de l'enfant ;
- Données psychosociales de l'enfant ;
- Données relatives à la famille d'origine ;
- Données relatives aux accueillants familiaux.

- Travailleurs salariés de l'institution :

La finalité du traitement est la gestion sociale et fiscale de travailleurs salariés dont la responsabilité finale incombe à l'employeur.

Les données récoltées sont classifiées comme suit :
- Données de sélection et recrutement ;
- Données d'identité ;
- Données administratives ;
- Données juridiques ;
- Données de contrôle d'accès.

- Membres et administrateurs de l'institution :

La finalité du traitement est le respect de la législation relative aux asbl et des obligations d'identification des membres et des administrateurs.

Les données récoltées sont classifiées comme suit :
- Données d'identité ;
- Données de contact et de compétence.

- Fournisseurs :

La finalité du traitement est de disposer des éventuelles données personnelles du contact le plus approprié chez le fournisseur en fonction de la demande.

Les données récoltées sont classifiées comme suit :
- Données d'identité.

- Partenaires :

La finalité du traitement est de disposer des éventuelles données personnelles du contact le plus approprié chez le partenaire en fonction de la demande.

Les données récoltées sont classifiées comme suit :
- Données d'identité.

Ces données personnelles ne sont jamais vendues à des tiers, pour quelque raison que ce soit.

Toute personne concernée par la récolte et le traitement de certaines de ces données personnelles peut prendre contact avec la direction de l'institution afin que celle-ci, en fonction de la demande, oriente la personne auprès du service compétent.

Les coordonnées de la direction sont les suivantes :
Ayumi OKAWA – 04/220.01.93 – 21 rue Forgeur, 4000 Liège

Vous trouverez également dans ce document la politique de l'institution en matière de sécurité informatique et de sécurité de l'information.

Pour l'élaboration de ce guide relatif à la sécurité des données personnelles, l'institution a veillé à élaborer, pour chaque registre de traitement de données à caractère personnel, une gestion des risques comprenant les éléments suivants :
- L'identification des impacts potentiels sur les droits et libertés des personnes concernées si l'un des événements suivants survient :
  - L'accès illégitime aux données personnelles ;
  - La modification non désirée de données personnelles ;
  - La disparition de données personnelles ;
- L'identification des sources de risques (qui ou quoi pourrait être à l'origine de chaque événement redouté) ;
- L'identification des menaces réalisables (qu'est-ce qui pourrait permettre que chaque événement redouté survienne) ;
- La détermination des mesures existantes ou prévues qui permettent de traiter ces risques ;
- La gravité et la vraisemblance de ces risques.

De cette analyse de gestion des risques, l'institution a mis en place la politique de sécurité reprise ci-dessous.

Sensibilisation des collaborateurs

Dès leur engagement et tout au long de leur parcours professionnel au sein de l'institution, les collaborateurs sont sensibilisés à l'importance du devoir de discrétion et de réserve, voire de secret professionnel dans la connaissance, la collecte et l'utilisation de données personnelles.

C'est ainsi que l'institution a notamment décidé de faire signer une clause de confidentialité aux travailleurs, toutes fonctions confondues.

Authentification des utilisateurs

Le service fonctionnant sur Office 365

Pour s'assurer que chaque utilisateur accède uniquement aux données dont il a besoin, l'institution dote chaque travailleur d'un identifiant qui lui est propre et veille à ce qu'il doive s'authentifier avant toute utilisation des moyens informatiques (mot de passe et log in).

L'organisme externe chargé de la sécurité informatique et la direction disposent des mots de passe et log in de l'ensemble du personnel. Le stockage des identifiants s'effectue de façon sécurisée.

Il existe une possibilité d'accès à distance via Office 365. Chaque utilisateur y accède via un identifiant qui lui est propre.

Gestion des habilitations

Le service fonctionnant sur Office 365

Chaque travailleur disposant d'un mot de passe et log in personnel n'a accès qu'aux seules données strictement nécessaires à l'accomplissement de ses missions.

Une double authentification 365 est mise en place pour assurer une sécurisation optimale des accès.

En cas de fin du contrat de travail, les mots de passe et log in sont désactivés immédiatement à leur départ.

Sécurisation des postes de travail

_____

Système antivirus, antispam, pare-feu et autre protection contre l'extérieur

L'institution a recours aux compétences techniques et informatiques d'un sous-traitant.

Celui-ci veille à protéger le système informatique de l'institution des intrusions externes en veillant à ce que le système réseau et/ou les ordinateurs bénéficient d'une protection optimale et mise à jour, en recourant aux systèmes les plus fiables se trouvant sur le marché.

L'institution se dote des protections les plus fiables présentes sur le marché. Elle veille à mettre à jour régulièrement ces systèmes de protection en se documentant périodiquement quant aux nouveautés en la matière.

Back up

Un back up de toutes les données se trouvant sur le réseau 365 est effectué une fois par jour.

Le sous-traitant informatique externe ainsi que la direction reçoivent une alerte au cas où ce back-up n'était pas effectué correctement ou que le contenu n'était pas lisible.

Autres mesures

L'institution veille à effacer, de façon sécurisée, les données présentes sur un poste de travail préalablement à sa réaffectation à une autre personne.

Sécurisation de l'informatique mobile

Seuls les moyens informatiques mobiles mis à disposition par l'institution peuvent être utilisés à des fins professionnelles.

Pour chaque type d'outil (PC portable, smartphone,…), des mesures de sécurité en termes d'accès au contenu (type verrouillage et déverrouillage) sont prévues par le responsable de la sécurité informatique.

La direction dispose d'une liste des outils informatiques mobiles. Il vérifie, de façon régulière, qu'aucune perte ou vol ne doit être déploré.

La reprise de ces outils informatiques mobiles, voire leur blocage, est géré par la direction.

Sauvegarde et prévention de la continuité d'activité

Le sous-traitant informatique externe dispose de la procédure à mettre en place en cas de disparition non désirée de données informatiques.

Le back up journalier des données du serveur 365 permet une remise en route de l'ensemble des activités de l'institution endéans les 24 heures.

Le sous-traitant et la direction reçoivent une alerte au cas où le back-up n'aurait pas été correctement effectué.

Archivage de manière sécurisée

L'institution a mis en place un archivage des données récoltées en version papier. Cet archivage s'effectue lorsque le service n'intervient plus dans la situation individuelle. Il s'effectue dans des armoires sécurisées au moyen d'une clé ou dans un lieu non accessible au public.

Encadrement de la maintenance

_____

Les interventions de maintenance confiées au sous-traitant informatique sont prévues dans le respect d'une clause de sécurité et de confidentialité, sous la responsabilité du service.

Les interventions de maintenance se déroulent sans que le sous-traitant informatique n'ait accès aux données personnelles récoltées.

Gestion de la sous-traitance

_____

En tant que responsable de traitement, l'institution peut faire appel à un sous-traitant qui, pour remplir les missions qui lui incombent, peut disposer de données personnelles traitées par le responsable de traitement.

Entre autres choses, l'institution, en tant que responsable de traitement, a recours à un sous-traitant :

- pour la gestion sociale, fiscale et comptable de l'institution ;

- pour le suivi informatique des bases de données de l'institution ;

Protection des locaux

_____

La sécurisation des locaux, que ce soit les endroits où se trouvent les serveurs ou les bureaux où se trouvent les données personnelle « version papier »,… est impérative.

Parmi les mesures prises, citons, à titre d'exemple:

- l'institution dispose d'une alarme incendie conforme aux normes de prévention incendie.

- les dossiers version papiers sont dans des armoires fermées à clé ou dans des lieux non accessibles au public.

Encadrement des développements informatiques

Il existe une base de données informatique relatives aux jeunes. Cette base de données est améliorée sur base d'un canevas vierge. En cas de problème spécifique sur la base de données, le sous-traitant apporte une solution au problème soit par le biais d'un accès à distance limité à son intervention et sous contrôle de la personne qui a demandé la résolution du problème, soit par le biais d'une capture d'écran indiquant le message d'erreur.

Droit des personnes dont des données personnelles ont été collectées et traitées

Toute personne ayant communiqué des données personnelles, y compris les travailleurs de l'institution pour leurs propres données, disposent des protections suivantes :

Droit d'accès et de rectification des données

A tout moment, vous pouvez prendre contact avec Ayumi Okawa, directrice (04.220.01.93) afin de connaître les données personnelles dont dispose l'institution et la façon dont ces données sont conservées. A ce droit d'accès est lié un droit de rectification s'il s'avère que ces données sont obsolètes.

Droit de portabilité

Chaque personne concernée a le droit, pour ce qui le concerne, de recevoir ses propres données dans un format structuré, couramment utilisé et lisible par une machine (PC).

Droit à l'effacement (ou droit à l'oubli numérique)

Toute personne concernée a le droit d'obtenir l'effacement de ses données dans les meilleurs délais dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités poursuivies ;
- les données ont fait l'objet d'un traitement illicite ;

Le droit à l'effacement ne concerne donc pas les données personnelles récoltées dans le cadre de la gestion sociale et fiscale des travailleurs salariés.

Désignation d'un délégué de protection des données (DPD ou DPO)

_____

La désignation d'un délégué à la protection des données (DPD) est obligatoire dans les cas suivants :

- le traitement des données à caractère personnel est effectué par une autorité publique ou un organisme public ;

- les activités de base du responsable de traitement consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées (profilage) ;

- les activités de base du responsable de traitement consistent en un traitement à grande échelle de catégories particulières de données (données sensibles).

L'institution n'est pas un organisme public. Elle ne collecte aucune donnée sensible à grande échelle et ne conserve les données personnelles que pour répondre adéquatement à ses missions et à son but social, sans aucune visée de profilage.

L'institution n'est donc pas tenue de disposer d'un délégué à la protection des données.

En raison de la petitesse de la structure, du peu de données personnelles récoltées et des moyens financiers disponibles, l'institution décide de ne pas engager de DPD.

L'institution veille toutefois à conscientiser, informer, former et suivre les travailleurs de l'institution collectant et traitant ces données personnelles.

Dernière mise à jour le 20 avril 2022