ASBL AQUARELLE
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 :

- 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 ;

- Volontaires :
- La finalité du traitement est le respect de la législation relative aux asbl et des obligations d'identification des volontaires.
  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 ;

- Bénéficiaires :
  La finalité du traitement est de garantir le suivi médical et les soisns périnataux à des femmes enceintes ou ayant accouché, sans protection sociale, en situation précaire ou psycho-socialement défavorisées.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
  - Données sociales ;
  - Données concernant la santé : données relatives à l'accouchement, surveillance des paramètres vitaus et obstétricaux, surveillance des plaies, surveillance des paramètres du nouveau-né,…

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 :
ASBL AQUARELLE
322 rue Haute
1000 Bruxelles
info@aquarelle-bru.be

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 entrée au sein de l'équipe d'aquarelle, 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.

Authentification des utilisateurs

Pour s'assurer que chaque utilisateur accède uniquement aux données dont il a besoin, chaque intervenant dispose d'un identifiant qui lui est propre et s'authentifie avant toute utilisation des moyens informatiques (mot de passe et log in).

Chaque intervenant n'a accès qu'aux seules données strictement nécessaires à l'accomplissement de ses missions.

Les éventuels stagiaires et étudiants effectuant un stage au sein de l'institution n'ont accès aux données personnelles que sous le contrôle direct d'un intervenant.

Un administrateur informatique externe dispose des différents identifiants. Le stockage des authentifiants s'effectue de façon sécurisée.

Traçage des accès et gestion des incidents

L'administrateur informatique externe a mis en place une procédure afin de pouvoir identifier un accès frauduleux, une utilisation abusive de données personnelles ou de déterminer l'origine d'un incident.

Sécurisation des postes de travail

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

L'administrateur informatique externe 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.

Back up

Option pour les institutions fonctionnant en réseau

Un back up de toutes les données se trouvant sur le réseau est effectué régulièrement.

L'administrateur informatique externe vérifie régulièrement que les back up sont effectués correctement et que le contenu est lisible.

Le back up est sauvegardé à l'extérieur de l'institution.

Autres mesures

La connexion de supports mobiles (clé USB, disque dur externe,…) n'est autorisée qu'avec l'accord préalable de la direction de l'institution. Il en va de même pour l'exécution d'applications téléchargées.

Seuls les moyens informatiques mobiles mis à disposition par l'institution peuvent être utilisés à des fins professionnelles. Aucune mise en réseau des données personnelles n'est prévue pour les smartphones.

Sécurisation des serveurs

La sécurisation des serveurs est réservée au service informatique externe qui dispose d'un accès dit « administrateur ».

Les opérations d'administration des serveurs s'effectuent via un réseau dédié et isolé, accessible après une authentification forte et avec une traçabilité renforcée.

Sécurisation du site internet

Le site internet ne comprend aucune donnée personnelle non librement consentie.

Sauvegarde et prévention de la continuité d'activité

La perte éventuelle des données personnelles n'entraverait pas la continuité d'activité, en effet, le service fonctionne sur la base du consentement explicite des bénéficiaires. Il suffira de réactiver ce consentement pour bénéficier à nouveau des données nécessaires à la réalisation du but social de l'institution.

Archivage et destruction des données

Les données sont conservées tant que les personnes concernées ne retirent pas leur consentement explicite ou tant qu'une législation impose la conservation des données, avec un maximum absolu de 30 ans (prescription dans le domaine de la santé).

La destruction des données informatiques est réalisée par l'administrateur informatique externe.

La destruction des données en version papier est réalisée sous la responsabilité de la direction via l'utilisation d'une déchiqueteuse.

Protection des locaux

Parmi les mesures mises en place, l'on peut citer :

- L'institution n'est accessible que par badge ou clé ;
- L'institution dispose de détecteurs de fumée ainsi que des moyens de lutte contre les incendies ;
- Les données en version papier sont conservées dans un endroit sécurisé (tant au niveau de l'armoire que du local).

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

Toute personne ayant communiqué des données personnelles disposent des protections suivantes :

<u>Droit d'accès et de rectification des données</u>

A tout moment, vous pouvez prendre contact avec Linda Doeraene, sage-femme directrice de l'asbl Aquarelle, 0479 40 92 10 et ou fonction et moyens de contact) afin de connaître les données personnelles dont dispose l'institution, 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) ;
- et si c'est techniquement possible, d'obtenir que les données soient directement transmises à un autre responsable de traitement (ceci ne vise que les données dont le responsable de traitement dispose en raison du consentement écrit de la personne concernée et pour lesquelles le traitement est effectué à l'aide de procédés automatisés).

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 ;
- elle retire le consentement sur lequel est fondé le traitement ;
- elle s'oppose au traitement de ses données à des fins de prospection ;
- les données ont fait l'objet d'un traitement illicite ;
- les données ont été collectées dans le cadre de l'offre directe de service à un enfant de moins de 13 ans.

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 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 intervenants de l'institution collectant et traitant ces données personnelles.

L'administrateur informatique externe dispose quant à lui d'un délégué à la protection des données.