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 :

- 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 d'équipement de protection individuelle ;
- 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 courriel de la direction sont les suivantes :
federation@aleap.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 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.

Authentification des utilisateurs

Chaque ordinateur est indépendant et chaque travailleur dispose de son code accès spécifique, créé par lui-même.

Il y a un ordinateur par poste de travail et dédié à un seul travailleur.

Il s'agit de PC fixes et/ou portables. Aucun accès aux données n'est prévu via internet.

Afin de garantir la continuité du service en cas d'absence d'un travailleur, un service informatique interne ou externe est seul habilité à, éventuellement, ouvrir l'accès de l'ordinateur à un autre travailleur.

Sécurisation des postes de travail

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

L'institution dispose de systèmes antivirus, pare-feu et antispam.

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 est réalisé par le service administratif sous la responsabilité de la direction ou une personne déléguée pour chaque ordinateur, fixe ou portable, de l'institution.

Chaque travailleur veillera à se conformer aux instructions données par le responsable informatique pour que ce back up se réalise à temps et à heure.

Ce back up est sauvegardé en un endroit considéré comme sûr par l'institution.

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, clé USB, ,…), des mesures de sécurité en termes d'accès au contenu sont prévues (code d'accès, limitation des données personnelles accessibles en fonction des tâches accessibles pour chaque travailleur salarié,...)

Le responsable de la sécurité informatique dispose d'une liste des outils informatiques mobiles, en lien avec les utilisateurs. 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 le responsable de la sécurité informatique.

Archivage de manière sécurisée

A ce jour, aucun archivage n'est réalisé, et ce pour les raisons suivantes :

- Le coût de l'archivage est disproportionné par rapport aux données privées récoltées ;
- Les données récoltées sont indispensables tout au long de la relation contractuelle avec les personnes visées et ne peuvent donc être archivées tant que la relation contractuelle perdure ;
- Les données récoltées sont par ailleurs nécessaires dans le cadre d'un contrôle du travail effectué par l'institution et/ou des subventions octroyées à l'institution et doivent donc rester disponibles tant que la prescription n'est pas atteinte.

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 et fiscale des travailleurs salariés de l'institution ;
- pour le suivi informatique de l'institution.

Cette relation avec le sous-traitant fait l'objet d'une convention qui clarifie les responsabilités respectives, la sécurisation des données personnelles tant auprès du responsable de traitement qu'auprès du sous-traitant, le nécessaire respect de la confidentialité,…

Protection des locaux

La sécurisation des locaux est impérative.

Parmi les mesures prises, l'on peut citer :

- L'institution a placé des alarmes anti-intrusion vérifiées périodiquement ;
- L'institution dispose de détecteurs de fumée ainsi que des moyens de lutte contre les incendies.

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 la direction via l'adresse federation@aleap. 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 ;

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