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 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 ;
- Affiliés formations :
  La finalité du traitement est de garantir aux affiliés un service conforme à leurs attentes et aux éventuelles obligations légales.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
- 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 ;
- Travailleurs salariés du responsable de traitement, client du service social :
  La finalité du traitement est d'aider le responsable du traitement, client du service social, à la gestion sociale, fiscale et comptable de ses travailleurs salariés.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité des travailleurs salariés ;
  - Données administratives ;
  - Données juridiques ;
  - Données comptables.

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 :
vinciane.schouppe@semafor.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.

C'est ainsi que l'institution inclut une clause de confidentialité dans les contrats de travail.

Authentification des utilisateurs

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).

Le travailleur chargé de la gestion informatique de la structure et la direction disposent des mots de passe et log in de l'ensemble du personnel. Le stockage des authentifiants s'effectue de façon sécurisée.

Gestion des habilitations

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.

Les éventuels stagiaires et étudiants effectuant un stage au sein de l'institution disposent, si le contenu du stage le justifie, d'un mot de passe et log in personnel limité à la durée de leur stage ou contrat.

En cas de fin du contrat de travail, les mots de passe et log in sont désactivés endéans les 24 heures.

Par ailleurs, chaque début d'année civile, une revue annuelle des habilitations est réalisée afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Toute information complémentaire relative à cette gestion des accès peut être obtenue auprès de la direction (voir adresse mail au début du document).

Traçage des accès et gestion des incidents

L'institution est en mesure de mettre 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.

Il existe une journalisation concernant les accès des utilisateurs en incluant leur identifiant, la date et l'heure de la connexion, la date et l'heure de la déconnexion.

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.

Back up

Option pour les institutions fonctionnant en réseau

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

La personne chargée de la sécurité informatique vérifie régulièrement que les back up sont effectués correctement et que le contenu est lisible.

Le back up est sauvegardé, via un sous-traitant, dans un cloud 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 du responsable interne et/ou externe de la sécurité informatique. Il en va de même pour l'exécution d'applications téléchargées.

Sécurisation des serveurs

La sécurisation des serveurs est réservée au service informatique (interne et 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.

L'institution dispose de systèmes de détection et prévention d'attaques spécifiques.

L'institution sous traite la conservation des données à un sous traitant qui dispose de serveurs dits miroirs et réalisent également des back up journaliers conservés, soit dans un endroit ignifuge et étanche, soit dans un lieu externe au siège sociale de l'institution. Le service informatique effectue un suivi régulier de ces back up.

Ces serveurs se trouvent dans un endroit sécurisé.

Sauvegarde et prévention de la continuité d'activité

_____

Le responsable du service informatique 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 permet une remise en route de l'ensemble des activités de l'institution endéans les 24 heures.

Le responsable externe de la sécurité informatique ou une personne déléguée teste régulièrement la restauration des sauvegardes.

Archivage de manière sécurisée

_____

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.

Encadrement de la maintenance et de la destruction des données

_____

Les interventions de maintenance confiées à un sous-traitant sont prévues dans le respect d'une clause de sécurité et de confidentialité, sous la responsabilité du service informatique de l'institution et du responsable de traitement.

La maintenance s'effectue directement sur le serveur avec un accès limité dans le temps.

Les interventions de maintenance sont transcrites dans un registre ad hoc.

Les données personnelles en version papier sont détruites en interne via un destructeur de papiers.

Les données personnelles en version informatique sont détruites, par chaque gestionnaire, sous la responsabilité des responsables interne et externe du service informatique.

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 l'encadrement et l'aide à apporter au service informatique interne.

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 …….. (nom, titre 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 16 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 travailleurs de l'institution collectant et traitant ces données personnelles.

Pour toute question…

Pour toute question relative au respect, par notre institution, du RGPD, vous pouvez contacter la direction à l'adresse courriel reprise en première page de ce document.

Vous pouvez également vous adresser à l'Autorité de Protection des Données, rue de la presse 35 à B-1000 Bruxelles – tel. 02/274.48.00.

Ce document détaillant notre politique de sécurité informatique et de l'information est un document unique dans nos rôles :

- de responsable de traitement ;
- de sous-traitant de nos clients dans nos missions de gestionnaire social et fiscal.

Veillez toutefois à vous adresser prioritairement au responsable de traitement de vos données personnelles.