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 ;

- **Clients commerciaux :**
  La finalité du traitement est de garantir aux clients commerciaux un service après vente conforme à leurs attentes et aux éventuelles obligations légales.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
  - Données relatives aux types de travaux réalisés ;

- **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 ;

- **Stagiaires CISP :**
  La finalité du traitement est de garantir le statut social est les droits sociaux du stagiaire.
  Les données récoltées sont classifiées comme suit :
  - Données d'identité ;
  - Données relatives au statut de la personne ;
  - Données psychosociales ;
  - Données administratives ;
  - Données d'équipement de protection individuelle.

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 :
Carole Duchâteau – Directrice adjointe du Germoir
Rue de Monceau-Fontaines, 42/3 – 6031 Monceau sur Sambre
Tel : 071 27 05 40

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 s'est dotée des outils suivants :

- Une charte informatique ;
- Des clauses de confidentialité prévues pour certains 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.

L'authentifiant reprend 8 caractères minimum et 4 types de caractères (majuscule, minuscule, chiffre, caractère spécial).

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 suspension du contrat de travail, les mots de passe et log in sont bloqués.

En cas de fin du contrat de travail, les mots de passe et log in sont désactivés endéans les 72 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 Carole Duchâteau et le fournisseur informatique Damnet.

Sécurisation des postes de travail

_____

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

Option pour les institutions fonctionnant avec un sous-traitant

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

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 de la sécurité informatique. Il en va de même pour l'exécution d'applications téléchargées.

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

Le responsable de la sécurité informatique dispose d'une liste des outils informatiques mobiles, en lien avec les utilisateurs, les mots de passe et log in. 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.

Protection du réseau informatique interne

Les précautions élémentaires suivantes sont préconisées par la CNIL :

- Limiter les accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.) ;
- Gérer les réseaux Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne ;
- Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.) ;
- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN ;
- Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Sécurisation des serveurs

La sécurisation des serveurs est réservée au service informatique 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 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.

Sécurisation du site internet

_____

Les précautions élémentaires suivantes sont préconisées par la CNIL :

- Mettre en œuvre le protocole TLS (en remplacement de SSL) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre ;
- Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques ;
- Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports ;
- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent ;
- Si des *cookies* non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du *cookie* ;
- Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

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 de la sécurité informatique ou une personne déléguée teste régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.

Archivage de manière sécurisée

_____

Dans le cadre de la mise en réseau des données, les données personnelles non nécessaires à l'exécution des missions de l'institution ne sont plus accessibles au personnel de l'institution.

Un archivage est effectué une fois par année civile. Cet archivage est conservé durant 10 ans débutant le 1er janvier de l'année suivant ledit archivage ou un délai plus long si certaines données archivées doivent être conservées en raison d'une action en justice (délai de prescription).

Le serveur sur lequel sont stockées les données archivées bénéficient des mêmes protection et mesures de sécurité informatique que les autres serveurs de l'institution.

L'accès aux données archivées ne peut s'effectuer que moyennant l'accord préalable du responsable du service informatique et du responsable du traitement des données.

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 convention avec ce sous-traitant prévoit également la destruction des données auxquelles le sous-traitant a éventuellement eu accès pour sa maintenance de la base de données utilisées par l'institution.

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

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 des bases de données 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, 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 « de base » possibles, l'on peut citer :

- L'institution a placé des alarmes anti-intrusion vérifiées périodiquement ;
- L'institution dispose des moyens de lutte contre les incendies ;
- La pièce réservée au serveur informatique et aux back up n'est accessible qu'aux personnes habilitées, avec traçabilité de leur passage et interventions ;

- Le matériel informatique dispose de moyens de protection spécifiques (exemples : système anti-incendie spécifique, surélévation de ce matériel contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation,…).

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 Carole DUCHATEAU – directrice adjointe - tel 071/27 05 40 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.