CNIL.

Fiche n° 10 - Comment assurer la sécurité des informations personnelles traitées par mon organisme ?

Un responsable de traitement doit prendre les mesures nécessaires pour préserver la sécurité et la confidentialité des données personnelles traitées, notamment en empêchant à des personnes non autorisées d'y accéder. Cela suppose d'assurer la sécurité des locaux, d'organiser les accès aux données, et de sensibiliser les personnes susceptibles d'y accéder.

Règles de droit

Un organisme doit assurer la sécurité et la confidentialité des données personnelles qu'il traite. Pour cela, **il doit mettre en place des mesures afin de limiter les risques d'atteinte à la confidentialité, la disponibilité et l'intégrité des données personnelles traitées.**

En pratique

Pour assurer la sécurité des données personnelles traitées, il doit mettre en place différentes mesures.

Mesures de sécurité physiques

Afin de sécuriser les locaux et plus particulièrement les salles hébergeant les serveurs informatiques et les différents éléments du réseau, un organisme doit définir et mettre en œuvre certaines mesures physiques adaptées telles que :

- le verrouillage des portes et des armoires,
- l'installation d'un système de vidéosurveillance, d'alarmes incendie ou d'alarmes anti-intrusion) afin de sécuriser les locaux.

Focus

Les documents papier contenant des informations personnelles doivent également faire l'objet de mesures de sécurité.

Mesures de sécurité logiques

Il est également nécessaire de définir et de mettre en œuvre des mesures de sécurité logiques et notamment :

1. *Sécuriser les postes de travail des salariés*

Pour cela, la structure pourrait :

- **chiffrer** les postes de travail ;
- **réaliser** des sauvegardes régulières des données, installer un verrouillage automatique des postes de travail après une courte période d'inactivité de l'utilisateur ;
- **limiter** le nombre de tentatives infructueuses d'accès à un compte utilisateur ;
- **installer** un pare-feu et un antivirus et les mettre régulièrement à jour.

2. *Tracer toutes les actions*

Pour cela, la structure pourrait par exemple :

- **procéder** au contrôle régulier des traces en utilisant des procédés de détection automatisés suspectes ;
- **enregistrer** les actions effectuées sur le système informatique pour une durée maximale de trois ans ;
- **prévoir** un système de journalisation.

3. *Gérer les habilitations*

La structure devra ainsi :

- **définir** des profils d'habilitation des utilisateurs ;
- **formaliser** une procédure de gestion des habilitations ;
- **contrôler** de manière régulière les habilitations.

Focus sur le secret professionnel

Dans la définition des habilitations, une structure devra porter une attention particulière aux données collectées par les personnes soumises au secret professionnel : les habilitations devront ainsi permettre de cloisonner ces données afin qu'elles ne soient pas divulguées.

Focus sur l'accès aux données des locataires par les gardiens

Les gardiens d'immeubles ont souvent des tâches différentes, ce qui a des conséquences quant à la nature des données auxquelles ils peuvent légitimement accéder.

Toutefois, ils ne doivent pas avoir accès à des données sans lien direct avec l'exercice de leurs missions (par exemple, un gardien d'immeuble qui, dans le cadre de ses missions, participe au recouvrement des loyers n'a pas à avoir accès aux données relatives à la situation financière des résidents).

4. *Authentifier les salariés*

Pour cela, il pourra être nécessaire d'adopter :

- un identifiant unique pour chaque salarié ;
- une politique rigoureuse de mots de passe pour l'accès aux postes de travail et à certains fichiers.

5. *Sécuriser l'archivage des données*

Une structure devra ainsi :

- **prévoir des copies de sauvegarde** des données à caractère personnel ;
- **sécuriser** de manière renforcée les sauvegardes concernant les données sensibles et celles relatives aux condamnations, infractions et mesures de sûreté.

Focus

Certains des salariés du bailleur social peuvent également être résidents de logements que l'organisme met à disposition.

Il faut alors être particulièrement vigilant afin de s'assurer que les informations relatives à l'attribution d'un logement n'apparaissent pas au sein du dossier RH de ses salariés bénéficiaires : une restriction des accès de leurs collègues à leur dossier locatif peut également être envisagée.

Focus concernant la mise en place de secteurs de gérance pour les gardiens d'immeubles

Pour être en mesure de répondre aux demandes des résidents en cas d'absence de leurs gardiens, certains bailleurs sociaux souhaitent étendre les profils d'habilitations pour tous les gardiens intervenant sur un même secteur de gérance.

Une telle extension est possible sous réserve de :

- **sensibiliser** les gardiens aux problématiques « Informatique et Libertés » ;
- **tracer** les accès afin d'identifier les accès frauduleux ou les utilisations abusives de données personnelles;
- **délimiter** le champ des données accessibles par les gardiens « remplaçants », en fonction de l'objet de la sollicitation ;
- **informer** oralement les résidents de manière individuelle et systématique dès lors qu'ils sollicitent une intervention :

> *« Pour pouvoir répondre immédiatement à votre requête, en lieu et place de M/Mme X (gardien) actuellement absent(e), je dois accéder à certaines de vos données. M'y autorisez-vous ou préférez-vous attendre son retour qui devrait intervenir d'ici X jours ? ».*

Mesures de sécurité organisationnelles

Pour garantir un niveau de sécurité suffisant, les mesures logiques ou physiques doivent être couplées à des mesures organisationnelles qui regroupent toutes les procédures à même d'assurer l'application des mesures de sécurité précitées et leur effectivité.

Une structure pourrait, par exemple, sensibiliser les salariés à la protection de la vie privée et des données personnelles en :

- annexant au règlement intérieur, une charte informatique afin d'informer et responsabiliser les salariés concernant les règles en matière de protection des données ;
- rappelant les bonnes pratiques « Informatique et Libertés » par des formations régulières.

À noter **:** Lorsqu'un organisme a recours à des prestataires extérieurs, il doit s'assurer d'encadrer contractuellement vos exigences en matière de sécurité. La responsabilité de l'organisme peut le cas échéant être engagée.

Pour se mettre en conformité

- **Etablir une charte informatique** rappelant les obligations de chacun ;
- **Mettre en œuvre** des mesures de sécurité physiques, logiques et organisationnelles ;
- **Sensibiliser les salariés** aux bonnes pratiques « Informatique et Libertés ».

Références

- Articles 32 à 35 du RGPD et guide de la sécurité des données personnelles (version 2024)
- Mots de passe : des recommandations de sécurité minimales pour les entreprises et les particuliers