FICHE N°10
SÉCURITÉ DES DONNÉES

L'article 34 de la loi « Informatique et Libertés » impose à un responsable de traitement de prendre toutes les précautions utiles pour préserver la sécurité des données dont il est responsable, en fonction de leur nature et des risques supposés. Il doit en particulier empêcher l'accès à ces données aux tiers non autorisés à les consulter.

Un bailleur social doit ainsi prendre un certain nombre de précautions lorsqu'il envisage de conserver, de communiquer ou de rendre accessibles des données à caractère personnel.

La sécurisation d'un système d'information exige de prendre en compte tous les aspects de sa gestion, tant au niveau organisationnel que technique, ainsi que réévaluer régulièrement les mesures initialement prises.

L'AUTHENTIFICATION DES UTILISATEURS

Le responsable d'un système informatique doit s'assurer que chaque utilisateur ne peut accéder qu'aux seules données dont il a besoin pour l'exercice de son activité.

Pour cela, chaque utilisateur doit disposer d'un identifiant unique et s'authentifier avant d'accéder au système.

Les mécanismes permettant d'authentifier les utilisateurs peuvent, par exemple, prendre la forme de mots de passe rattachés à un identifiant ou à une carte à puce.

Les identifiants des utilisateurs doivent être différents des comptes définis par défaut par les éditeurs de logiciels.

Lorsque l'authentification ou l'identification des utilisateurs est assurée par de mots de passe, la CNIL considère que ceux-ci doivent être constitués d'au moins huit caractères, à choisir parmi trois types différents (majuscules, minuscules, chiffres, caractères spéciaux), et être régulièrement renouvelés, par exemple tous les six mois.

PRÉCISIONS

Les mots de passe des comptes définis par défaut par les éditeurs doivent être modifiés par les utilisateurs, dès leur première connexion.

Aucun compte usager ne doit être partagé entre plusieurs utilisateurs.

LA GESTION DES HABILITATIONS

Chaque utilisateur ne devant accéder qu'aux données strictement nécessaires à l'exercice de son activité professionnelle, des profils d'habilitation doivent être définis pour déterminer les types de données accessibles à une catégorie d'utilisateur.

Une procédure de gestion des habilitations doit être formalisée afin d'assurer leur mise à jour, notamment pour supprimer les permissions d'accès des utilisateurs qui ne sont plus habilités ou qui ont quitté l'organisme.

Cette procédure doit également prévoir des contrôles des habilitations afin de s'assurer que les permissions d'accès aux données ne sont pas détournées (par exemple, partage d'un seul compte utilisateur utilisé par différentes personnes).

SENSIBILISATION DES UTILISATEURS ET FORMALISATION DES RÈGLES DE SÉCURITÉ

Une charte informatique, qui doit être annexée au règlement intérieur, peut être rédigée afin d'informer et responsabiliser les usagers, notamment sur les points suivants :

- **Le rappel des règles de protection des données** et les sanctions encourues en cas de non respect de la loi.
- **Le champ d'application de la charte**, qui inclut notamment :
  - les modalités d'intervention du service de l'informatique interne, notamment en cas de télémaintenance ;
  - les moyens d'authentification ;
  - les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple de :
  - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
  - ne jamais confier son moyen d'authentification à un tiers (identifiant/mot de passe, carte à puce et code PIN, etc.) ;
  - ne pas modifier les paramétrages du poste de travail ;
  - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
  - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
  - ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;
  - définir les modalités de copie de données sur un support externe ;
  - sensibiliser sur les risques d'hameçonnage (« *phishing* ») et autres méthodes d'acquisition déloyale d'information ;
  - sécuriser les outils personnels utilisés dans un cadre professionnel (BYOD).
- **Les modalités d'utilisation des moyens informatiques et de télécommunications** mis à disposition comme :
  - le poste de travail ;
  - les équipements nomades ;
  - l'espace de stockage individuel ;
  - le réseau local ;
  - Internet ;
  - la messagerie électronique ;
  - le téléphone.
- **Les conditions d'administration du système d'information**, et l'existence, le cas échéant, de :
  - systèmes automatiques de filtrage des accès aux matériels et aux applications ;
  - systèmes automatiques de traçabilité ;
  - gestion du poste de travail.
- **Les responsabilités et sanctions encourues en cas de non respect de la charte.**

LA SÉCURITÉ DES POSTES DE TRAVAIL

La sécurité des postes de travail implique notamment des mesures permettant de prévenir les tentatives d'accès frauduleux, l'exécution d'un virus ou la prise de contrôle à distance, notamment par Internet.

Il est ainsi conseillé de limiter le nombre de tentatives infructueuses d'accès à un compte utilisateur. En fonction du contexte (nature des données, nombre de dossiers accessibles, etc.), le nombre de tentatives

autorisées par le système peut varier de cinq à dix. Lorsque la limite est atteinte, le compte en question doit être bloqué, temporairement ou jusqu'à l'intervention d'un administrateur du système.

Il est également conseillé d'installer un pare-feu logiciel (firewall), pour contrôler les communications entrantes et sortantes, ainsi que de limiter les ports logiciels de communication à ceux qui sont strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail (par exemple le port 80 pour l'accès http à Internet, le port 443 pour l'accès https, etc.).

Les antivirus ainsi que tous les autres logiciels utilisés doivent être régulièrement mis à jour.

Un verrouillage automatique des sessions à l'issue d'une période d'inactivité permet d'améliorer la sécurité globale du système. S'agissant de l'accès à une application métier, la fermeture d'une session après cinq minutes d'inactivité permet d'améliorer la sécurité sans entraîner de gène excessive dans l'activité de l'utilisateur.

LES MESURES DE SAUVEGARDES ET L'ARCHIVAGE

Des copies de sauvegarde des données à caractère personnel peuvent être effectuées, conformément à une politique de sauvegarde.

Une sécurisation renforcée est requise pour les sauvegardes des données sensibles ou jugées confidentielles par l'organisme (par exemple par une mesure de chiffrement ou une traçabilité renforcée des accès et des opérations effectuées sur les sauvegardes).

Concernant les possibilités de conservation des données, on distingue habituellement trois catégories de stockage :

- **Les bases actives :** les données d'utilisation courante par les services en charge de la mise en œuvre du traitement,
- **Les archives intermédiaires :** les données qui ne sont plus utilisées mais présentant encore un intérêt administratif pour l'organisme (par exemple le temps d'une prescription). Ces données sont conservées de manière distincte et leur consultation doit être ponctuelle et motivée, par des personnes spécifiquement habilitées.
- **Les archives définitives :** les données présentant un intérêt historique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction (par exemple, le cas d'archives pour le compte de l'État). Ces archives doivent également faire l'objet de mesures spécifiques visant à assurer leur intégrité.

Par ailleurs, une sauvegarde des logiciels servant au traitement peut être également prévue afin de garantir la pérennité de ce dernier.

RAPPEL

Les archives doivent être sécurisées et chiffrées si les données archivées sont des données sensibles ou jugées confidentielles par l'organisme.

LA MAINTENANCE

Lors de la maintenance et des interventions techniques, la sécurité des données doit être garantie. La confidentialité des données peut être garantie en prévoyant par exemple d'enregistrer les interventions de maintenance dans une main courante et d'encadrer les interventions effectuées par un responsable de l'organisme.

En cas d'assistance sur les postes de travail, les outils d'administration à distance doivent être configurés de manière à recueillir l'accord de l'utilisateur avant toute interven-

tion sur son poste, par exemple en cliquant sur une icône ou en répondant à un message s'affichant à l'écran. L'utilisateur doit également pouvoir constater si la prise en main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

Les données présentes sur les matériels destinés à être mis au rebut doivent être supprimées par une procédure d'effacement sécurisé ou par une destruction physique du matériel. Par conséquent, une inspection du matériel doit être effectuée pour s'assurer que toute donnée a bien été supprimée de façon sécurisée.

LA TRAÇABILITÉ

Afin d'être en mesure d'identifier a posteriori un accès frauduleux à des données personnelles, une utilisation abusive de telles données ou de déterminer l'origine d'un incident, il convient d'enregistrer les actions effectuées sur le système informatique.

Le système doit ainsi enregistrer les événements (accès à l'application, accès et opérations sur les données), garantir que ces enregistrements ne peuvent être altérés et conserver ces éléments pendant une durée non excessive. Ces événements sont composés de traces fonctionnelles (traces relatives au fonctionnement de l'application métier), de traces techniques (traces relatives au fonctionnement des éléments réseau et système mis en œuvre sur le système d'information) et de traces embarquées (traces inscrites dans des documents, par exemple, pour en certifier l'origine).

À cet effet, il peut être nécessaire de prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers de logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les événements sur une période glissante ne pouvant excéder six mois (sauf obligation légale ou autorisation par la CNIL).

Il faudra dans ce cas prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. En cas d'opérations effectuées sur les données sensibles, il est nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que par exemple les données consultées ou modifiées. Par ailleurs, les données de journalisation ne doivent être utilisées que pour leur finalité annoncée d'identification a posteriori en excluant toute autre finalité comme par exemple le contrôle des horaires ou la vérification du travail effectué. Dans tous les cas, ces traces devront être régulièrement analysées afin de détecter tout comportement suspect ou anormal.

L'ÉCHANGE D'INFORMATION AVEC D'AUTRES ORGANISMES

La communication de données à caractère personnel doit être sécurisée. La messagerie électronique et le fax, même s'ils apportent un gain de temps, ne constituent pas a priori un moyen de communication sûr pour transmettre des données personnelles. Une simple erreur de manipulation peut conduire à la divulgation d'informations personnelles à des destinataires non habilités et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, la transmission via Internet de données nominatives comporte, compte tenu de l'absence générale de confidentialité du

réseau Internet, des risques importants de divulgation de ces données et d'intrusion dans les systèmes informatiques internes par exploitation de ces données frauduleusement acquises.

Dans tous les cas, la transmission du secret (clé de déchiffrement, mot de passe, etc.) garantissant la confidentialité du transfert doit s'effectuer de manière distincte, si possible via un canal de nature différente (par exemple, envoi d'un fichier chiffré par courriel et communication du mot de passe par SMS).

Concernant la confidentialité d'une communication, il est possible de chiffrer directement les données ou le canal de transmission lors d'un envoi via un réseau. En cas de transfert matériel (copie sur DVD ou clé USB par exemple), les données peuvent être chiffrées préalablement à leur enregistrement sur le support physique. Si une transmission utilise la messagerie électronique, le chiffrement des pièces à transmettre est alors indispensable. Si les document transmis par voie électronique n'est pas chiffré, il sera alors indispensable de chiffrer le canal de transmission. A cet effet, l'utilisation du protocole SSL/TLS garantit l'authentification des serveurs (ainsi qu'éventuellement celle des clients) et la confidentialité des communications (SFTP pour le transfert de fichiers ou HTTPS pour les services Web sont des protocoles de transmission sécurisée).

PRÉCISION

Un portail sécurisé, sous la forme d'un service Web associé à l'utilisation du protocole SSL, garantit la confidentialité des échanges de données entre divers organismes. Un tel portail associé à l'identification des usagers permet également de limiter l'accès aux données aux seules personnes habilitées.

L'ANONYMISATION

Le terme d'anonymisation est réservé aux opérations irréversibles. On utilise le terme de pseudonymisation lorsque l'opération est réversible.

Une anonymisation irréversible consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées, rendant impossible toute ré-identification des personnes.

La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. Cette technique permet la ré-identification ou l'étude de corrélations en cas de besoin particulier.

Lors d'une pseudonymisation, il faut être vigilant dans la mesure où une ré-identification peut intervenir à partir d'informations partielles (par exemple, la combinaison des données ville et date de naissance peut être suffisante).

Exemple de pseudonymisation :
Une pseudonymisation limitant efficacement le risque de ré-identification directe peut par exemple être effectuée en générant une clé secrète longue et difficile à mémoriser (une combinaison de caractères aléatoires), puis en appliquant une fonction dite à sens unique sur les données (par exemple, un algorithme de hachage à clé secrète tel HMAC). En l'absence de besoin de ré-identification efficace, la clé secrète peut être supprimée pour diminuer le risque de ré-identification. Si la conservation de la clé secrète est nécessaire, des mesures doivent être mises en place pour assurer la confidentialité de cette clé, il est notamment conseillé de tracer les accès à cette clé. La clé secrète devra être suffisamment complexe pour ne pas affaiblir le processus d'anonymisation.

FICHE N°10

SÉCURITÉ DES DONNÉES

LE CHIFFREMENT

Le chiffrement, parfois improprement appelé cryptage, est un procédé cryptographique permettant de garantir la confidentialité d'une information. D'autres mécanismes de cryptographie permettent d'assurer d'autres propriétés de sécurité, par exemple l'intégrité et l'authenticité d'un message en le signant.

De manière générale, on distingue la cryptographie symétrique où une seule clé est nécessaire (la même clé sert alors à chiffrer et à déchiffrer), de la cryptographie asymétrique dans laquelle on utilise une paire de clé : une clé publique, pouvant être connue de n'importe qui, et une clé privée dont la confidentialité doit être strictement encadrée. Dans ce deuxième cas, une clé servira à chiffrer (clé publique) et une clé secrète (différente de la clé publique) servira à déchiffrer (clé privée).

L'intérêt de la cryptographie asymétrique est multiple. Dans ce cas, chaque personne n'a besoin que d'une paire de clés privée/publique, à la différence d'un chiffrement symétrique où il est nécessaire d'avoir autant de clés différentes que de couples de personnes voulant communiquer de manière confidentielle. Cependant le chiffrement symétrique est reconnu comme étant plus rapide.

Pour identifier les algorithmes et les paramètres à utiliser en cryptographie, les annexes B1 et B2 du Référentiel Général de Sécurité peuvent être utilisées. D'un point de vue opérationnel, l'ANSSI certifie et qualifie différents produits de sécurité qui respectent, voir dépassent, ces critères.

Concernant le chiffrement symétrique, il pourra s'agir, à l'heure actuelle, d'AES avec des clés de longueur au moins égale à 128 ou 256 bits générées par des logiciels éprouvés et régulièrement mis à jour (par exemple OpenSSL). Concernant le chiffrement asymétrique, il pourrait d'agir de RSA (plus précisément celui de PKCS#1) en utilisant des modules et des clés de longueur au moins égale à 2048 bits.

PRÉCISION

Pour les échanges intervenant entre les divers acteurs du logement social, le chiffrement des communications et des données peut s'effectuer au moyen de chiffrements symétriques ou asymétriques.

Un chiffrement symétrique permet d'utiliser une seule et même clé pour chiffrer et déchiffrer un message. Toutefois il est nécessaire d'avoir autant de clés différentes que de couples de personnes voulant communiquer de manière confidentielle. Il est également nécessaire de transmettre la clé par un vecteur de communication différent de celui utilisé pour transmettre le fichier chiffré.

Un chiffrement asymétrique nécessite une clé servant à chiffrer (clé publique) et une clé servant à déchiffrer (clé privée). Ce mode de chiffrement est intéressant lorsque les échanges interviennent entre de multiples acteurs. En effet, un message émis pourra être chiffré par la clé publique connue de tous mais ne sera déchiffrable que par les destinataires connaissant la clé privée.