LES GUIDES DE LA CNIL - ÉDITION 2017

# LA SÉCURITÉ DES DONNÉES PERSONNELLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

# LA SÉCURITE DES DONNÉES PERSONNELLES

SOMMAIRE

# INTRODUCTION

La gestion des risques permet de déterminer les précautions à prendre « ***au regard de la nature des données et des risques*** *présentés par le traitement, pour préserver la sécurité des données* » (article 34 de la loi du 6 janvier 1978 modifiée, dite loi « Informatique et Libertés »). Le règlement européen 2016/679 du 27 avril 2016 (dit « règlement général sur la protection des données » ou RGPD) précise que la protection des données personnelles nécessite de prendre des « *mesures techniques et organisationnelles appropriées afin de garantir un* ***niveau de sécurité adapté au risque*** » (article 32).

Une telle approche permet en effet une prise de décision objective et la détermination de mesures strictement nécessaires et adaptées au contexte. Il est cependant parfois difficile, lorsque l'on est pas familier de ces méthodes, de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été mis en oeuvre.

Pour vous aider dans votre mise en conformité, **ce guide rappelle ces précautions élémentaires qui devraient être mises en œuvre de façon systématique.**

**Dans l'idéal, ce guide sera utilisé dans le cadre d'une gestion des risques, même minimale, constituée des quatres étapes suivantes :**

**Recenser les traitements** de données à caractère personnel, automatisés ou non, les données traitées *(ex : fichiers client, contrats) et les supports sur lesquels elles reposent :*

- les matériels (ex : serveurs, ordinateurs portables, disques durs) ;
- les logiciels (ex : système d'exploitation, logiciel métier) ;
- les canaux de communication (ex : fibre optique, Wi-Fi, Internet) ;
- les supports papier (ex : document imprimé, photocopie).

**Apprécier les risques** engendrés par chaque traitement :

1. **Identifier les impacts potentiels** sur les droits et libertés des personnes concernées, pour les trois évènements redoutés suivants :
   - **accès illégitime à des données** (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
   - **modification non désirée de données** (ex : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès) ;
   - **disparition de données** (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).

2. **Identifier les sources de risques** (qui ou quoi pourrait être à l'origine de chaque évènement redouté ?), en prenant en compte des sources humaines internes et externes (ex : administrateur informatique, utilisateur, attaquant externe, concurrent), et des sources non humaines internes ou externes (ex : eau, matériaux dangereux, virus informatique non ciblé).

3. **Identifier les menaces réalisables** (qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :
   - utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;
   - modifiés (ex : piégeage logiciel ou matériel – *keylogger*, installation d'un logiciel malveillant) ;
   - perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;
   - observés (ex : observation d'un écran dans un train, géolocalisation d'un matériel) ;
   - détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;
   - surchargés (ex : unité de stockage pleine, attaque par dénis de service).

4. **Déterminer les mesures existantes ou prévues** qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

5. **Estimer la gravité et la vraisemblance** des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

Le tableau suivant peut être utilisé pour formaliser cette réflexion :

| Risques | Impacts sur les personnes | Principales sources de risques | Principales menaces | Mesures existantes ou prévues | Gravité | Vraisemblance |
|---|---|---|---|---|---|---|
| Accès illégitime à des données | | | | | | |
| Modification non désirée de données | | | | | | |
| Disparition de données | | | | | | |

**Mettre en œuvre et vérifier les mesures prévues.** Si les mesures existantes et prévues sont jugées appropriées, il convient de s'assurer qu'elles soient appliquées et contrôlées.

**Faire réaliser des audits de sécurité périodiques.** Chaque audit devrait donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.

## POUR ALLER PLUS LOIN

- Le RGPD introduit la notion d' « *analyse d'impact relative à la protection des données* » et précise que celle-ci doit au moins contenir « *une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité, une appréciation des risques [...] et les mesures envisagées pour traiter ces risques et se conformer au règlement* » (voir article 35.7). **La réflexion sur les risques dont il est question dans la présente fiche permet d'alimenter le volet sur l'appréciation des risques de l'analyse d'impact.**
- Les guides PIA de la CNIL (https://www.cnil.fr/fr/PIA-privacy-impact-assessment) permettent de mener une analyse d'impact relative à la protection des données.
- **L'étude des risques sur la sécurité de l'information**[1] **peut être menée en même temps que l'étude des risques sur la vie privée**. Ces approches sont compatibles.
- L'étude des risques permet de déterminer des mesures de sécurité à mettre en place. Il est nécessaire de **prévoir un budget** pour leur mise en œuvre.

1 Par exemple à l'aide de la méthode EBIOS, méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) du Secrétariat général de la défense et de la sécurité nationale (SGDSN). EBIOS est une marque déposée du SGDSN (https://www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/).

# 1 SENSIBILISER LES UTILISATEURS

## Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Sensibiliser les utilisateurs travaillant avec des données à caractère personnel aux risques liés aux libertés et à la vie privée,** les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement. Organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique, etc.
- **Documenter les procédures d'exploitation,** les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données à caractère personnel, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.
- **Rédiger une charte informatique et lui donner une force contraignante** (ex. annexion au règlement intérieur). Cette charte devrait au moins comporter les éléments suivants :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non respect de celles-ci.
2. Le champ d'application de la charte, qui inclut notamment :
   - les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
   - les moyens d'authentification utilisés par l'organisme ;
   - les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment 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 identifiant/mot de passe à un tiers ;
     - 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 si cela ne relève pas des tâches incombant à l'utilisateur ;
     - respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.
3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :
   - le poste de travail ;
   - les équipements nomades (notamment dans le cadre du télétravail) ;
   - les espaces de stockage individuel ;
   - les réseaux locaux ;
   - les conditions d'utilisation des dispositifs personnels ;
   - l'Internet ;
   - la messagerie électronique ;
   - la téléphonie.

# 1 SENSIBILISER LES UTILISATEURS

**4.** Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :
- systèmes automatiques de filtrage ;
- systèmes automatiques de traçabilité ;
- gestion du poste de travail.

**5.** Les responsabilités et sanctions encourues en cas de non respect de la charte.

## POUR ALLER PLUS LOIN

- Mettre en place une politique de **classification de l'information** définissant plusieurs niveaux et imposant un marquage des documents et des e-mails contenant des données confidentielles.
- Porter une mention visible et explicite sur chaque page des documents papier ou électroniques qui contiennent des données sensibles[2].
- Organiser des séances de formation et de sensibilisation à la sécurité de l'information. Des rappels périodiques peuvent être effectués par le biais de la messagerie électronique.
- Prévoir la signature d'un **engagement de confidentialité** (voir modèle de clause ci-dessous), ou prévoir dans les contrats de travail une **clause de confidentialité spécifique** concernant les données à caractère personnel.

### Exemple d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel :

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____
(ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :
- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires

Nom :
Signature :


2 Les données sensibles sont décrites à l'article 8 de la loi informatique et libertés, et à l'article 9 du RGPD.

2

# AUTHENTIFIER LES UTILISATEURS

## Reconnaître ses utilisateurs pour pouvoir ensuite leur donner les accès nécessaires.

Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un **identifiant qui lui est propre** et doit **s'authentifier** avant toute utilisation des moyens informatiques.

Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés selon qu'ils font intervenir :
- **ce que l'on sait,** par exemple un mot de passe ;
- **ce que l'on a,** par exemple une carte à puce ;
- **une caractéristique qui nous est propre,** par exemple une empreinte digitale, ou la manière de tracer une signature manuscrite. Pour rappel, la loi informatique et libertés subordonne l'utilisation de la biométrie à l'autorisation préalable de la CNIL[3].

L'authentification d'un utilisateur est qualifiée de forte lorsqu'elle a recours à une combinaison d'au moins deux de ces catégories.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Définir un identifiant unique par utilisateur et interdire les comptes partagés** entre plusieurs utilisateurs. Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, exiger une validation de la hiérarchie et mettre en œuvre des moyens pour les tracer.
- **Respecter la recommandation de la CNIL[4] dans le cas d'une authentification des utilisateurs basée sur des mots de passe,** notamment en stockant les mots de passe de façon sécurisée et en applicant les règles de complexité suivantes pour le mot de passe :
  - au moins 8 caractères comportant 3 des 4 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux) si l'authentification prévoit une restriction de l'accès au compte (cas le plus courant) comme :
    - une temporisation d'accès au compte après plusieurs échecs ;
    - un « Captcha » ;
    - un verrouillage du compte après 10 échecs ;
  - **12 caractères minimum et 4 types de caractères** si l'authentification repose uniquement sur un mot de passe ;
  - **plus de 5 caractères** si l'authentification comprend une information complémentaire. L'information complémentaire doit utiliser **un identifiant confidentiel d'au moins 7 caractères** et bloquer le compte à la 5ème tentative infructueuse ;
  - le mot de passe peut ne faire que **4 caractères** si l'authentification s'appuie sur un matériel détenu par la personne et si le mot de passe n'est utilisé que pour déverrouiller le dispositif matériel détenu en propre par la personne (par exemple une carte à puce ou téléphone portable) et qui celui-ci se bloque à la 3ème tentative infructueuse.

Des moyens mnémotechniques permettent de créer des mots de passe complexe, par exemple :
- en ne conservant que les premières lettres des mots d'une phrase ;
- en mettant une majuscule si le mot est un nom (ex : Chef) ;
- en gardant des signes de ponctuation (ex : ') ;
- en exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un → 1) ;
- en utilisant la phonétique (ex : acheté → ht).

Exemple, la phrase « *un **C**hef d'**E**ntreprise **a**verti en vaut deux* » peut correspondre au mot de passe **1Cd'Eaev2.**

3 À ce sujet, consulter l'article dédié « Biométrie : un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail » sur notre site web https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail
4 https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

# 2 AUTHENTIFIER LES UTILISATEURS

Obliger l'utilisateur à changer, dès sa première connexion, tout mot de passe **attribué par un administrateur ou automatiquement** par le système lors de la création du compte ou d'un renouvellement consécutif à un oubli.

## CE QU'IL NE FAUT PAS FAIRE

- Communiquer son mot de passe à autrui.
- Stocker ses mots de passe dans un fichier en clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
- Enregistrer ses mots de passe dans son navigateur sans mot de passe maître.
- Utiliser des mots de passe ayant un lien avec soi (nom, date de naissance, etc.).
- Utiliser le même mot de passe pour des accès différents.
- Conserver les mots de passe par défaut.
- S'envoyer par e-mail ses propres mots de passe.

## POUR ALLER PLUS LOIN

- **Privilégier l'authentification forte** lorsque cela est possible.
- **Limiter le nombre de tentatives d'accès** aux comptes utilisateurs sur les postes de travail et bloquer temporairement le compte lorsque la limite est atteinte.
- **Imposer un renouvellement du mot de passe** selon une périodicité pertinente et raisonnable.
- Mettre en œuvre des moyens techniques pour **faire respecter les règles relatives à l'authentification** (par exemple : blocage du compte en cas de non renouvellement du mot de passe).
- Éviter, si possible, que les identifiants (ou logins) des utilisateurs soient ceux des comptes définis par défaut par les éditeurs de logiciels et désactiver les comptes par défaut.
- **Utiliser des gestionnaires de mots de passe pour avoir des mots de passe différents pour chaque service,** tout en ne retenant qu'un mot de passe maître (https://www.cnil.fr/fr/construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces).
- **Stocker les mots de passe de façon sécurisée** au minimum hachés avec une fonction de hachage cryptographique utilisant un sel ou une clé, et au mieux transformés avec une fonction spécifiquement conçue à cette fin utilisant toujours un sel ou une clé[5] (*voir Fiche 17*). Une clé ne doit pas être stockée dans la même base de données que les empreintes.
- Se référer aux *règles et recommandations concernant les mécanismes d'authentification* publiées par l'ANSSI dès lors que des mécanismes d'authentification forte sont mis en œuvre, notamment ses annexes B3[6] et B1[7] s'agissant respectivement des *mécanismes d'authentification* et des *mécanismes cryptographiques*.

5 On appelle « sel » l'aléa utilisé lorsqu'il est différent pour chaque mot de passe stocké et « clé » lorsque l'aléa utilisé est commun à la transformation d'un ensemble de mots de passe (par exemple toute une base de données).
6 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf.
7 https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf.

3

# GÉRER LES HABILITATIONS

## Limiter les accès aux seules données dont un utilisateur a besoin.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Définir des profils d'habilitation** dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.
- **Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat.**
- **Réaliser une revue annuelle des habilitations** afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

### CE QU'IL NE FAUT PAS FAIRE

- Créer ou utiliser des comptes partagés par plusieurs personnes.
- Donner des droits d'administrateurs à des utilisateurs n'en ayant pas besoin.
- Accorder à un utilisateur plus de privilèges que nécessaire.
- Oublier de retirer des autorisations temporaires accordées à un utilisateur (pour un remplacement, par exemple).
- Oublier de supprimer les comptes utilisateurs des personnes ayant quitté l'organisation ou ayant changé de fonction.

### POUR ALLER PLUS LOIN

Établir, documenter et réexaminer régulièrement **une politique de contrôle d'accès** en rapport avec les traitements mis en œuvre par l'organisation qui doit inclure :

- les procédures à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'une personne ayant accès aux données à caractère personnel ;
- les conséquences prévues pour les personnes ayant un accès légitime aux donnés en cas de non-respect des mesures de sécurité ;
- les mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement (*voir Fiche n°4 : Tracer les accès et gérer les incidents*).

4

# TRACER LES ACCÈS ET GÉRER LES INCIDENTS

## Tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).

Afin de pouvoir **identifier un accès frauduleux** ou une **utilisation abusive** de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit **enregistrer les évènements pertinents** et **garantir que ces enregistrements ne peuvent être altérés.** Dans tous les cas, il ne faut **pas conserver ces éléments pendant une durée excessive.**

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Prévoir un système de journalisation** (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « *logs* ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité :
  - ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ;
  - **la journalisation doit concerner, au minimum, les accès des utilisateurs** en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ;
  - dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné.
- **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des représentants du personnel.
- **Protéger les équipements de journalisation et les informations journalisées** contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée.
- Établir des procédures détaillant la surveillance de l'utilisation du traitement et **examiner périodiquement les journaux d'événements** pour y détecter d'éventuelles anomalies.
- Assurer que **les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement.**
- **Notifier toute violation de données à caractère personnel à la Cnil et,** sauf exception prévue par le RGPD[8], **aux personnes concernées** pour qu'elles puissent en limiter les conséquences.

### CE QU'IL NE FAUT PAS FAIRE

- Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique (par exemple, utiliser les traces pour compter les heures travaillées est un détournement de finalité, puni par la Loi).

### POUR ALLER PLUS LOIN

- Voir les recommandations de sécurité pour la mise en œuvre d'un système de journalisation publiées par l'ANSSI : https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/

8 articles 33 et 34 du RGPD

# 5 SÉCURISER LES POSTES DE TRAVAIL

## Prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment via Internet.

Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d'entrée

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- Prévoir un mécanisme de **verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné.
- Installer un **« pare-feu »** (« *firewall* ») logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
- Utiliser des **antivirus régulièrement mis à jour** et prévoir une politique de **mise à jour régulière des logiciels**
- Configurer les logiciels pour que les **mises à jour de sécurité se fassent automatiquement** dès que cela est possible.
- **Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme** plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.
- **Limiter la connexion de supports mobiles** (clés USB, disques durs externes, etc.) à l'indispensable.
- Désactiver l'exécution automatique (« *autorun* ») depuis des supports amovibles.

  Pour l'**assistance sur les postes de travail :**
  - les outils d'administration à distance doivent **recueillir l'accord** de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran ;
  - l'utilisateur doit également pouvoir **constater si la prise de main à distance est en cours** et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

### CE QU'IL NE FAUT PAS FAIRE

- Utiliser des systèmes d'exploitation obsolètes (voir la liste à http://www.cert.ssi.gouv.fr/site/CERTA-2005-INF-003).
- Donner des droits administrateurs aux utilisateurs n'ayant pas de compétences en sécurité informatique.

### POUR ALLER PLUS LOIN

- **Interdire l'exécution d'applications téléchargées** ne provenant pas de sources sûres.
- **Limiter l'usage** d'applications nécessitant des droits de niveau administrateur pour leur exécution.
- **Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation** à une autre personne.
- **En cas de compromission d'un poste, rechercher la source ainsi que toute trace d'intrusion** dans le système d'information de l'organisme, pour détecter la compromission d'autres éléments.
- **Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d'information de l'organisme**. Le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, publie sur son site web (http://cert.ssi.gouv.fr/) des alertes et des avis sur les vulnérabilités découvertes dans des logiciels et matériels et donne, lorsque cela est possible, des moyens pour s'en prémunir.
- **Mettre à jour les applications** lorsque des failles critiques ont été identifiées et corrigées.
- Installer les **mises à jour critiques des systèmes d'exploitation** sans délai en programmant une vérification automatique hebdomadaire.
- Diffuser à tous les utilisateurs **la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un événement inhabituel** touchant aux systèmes d'information et de communication de l'organisme.
- Consulter la note du CERT-FR sur les bons réflexes en cas d'intrusion sur un système d'information, accessible à l'adresse http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html.

# 6 SÉCURISER L'INFORMATIQUE MOBILE

## Anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.

La multiplication des ordinateurs portables, des clés USB et des *smartphones* rend indispensable d'anticiper les atteintes à la sécurité des données consécutives au vol ou à la perte de tels équipements.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles** (ex : vol de matériel) et aux procédures prévues pour les limiter.
- **Mettre en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation** des postes nomades, pour se prémunir contre la disparition des données stockées.
- **Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles** (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.), par exemple :
  - le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ;
  - le chiffrement fichier par fichier ;
  - la création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés.

  De nombreux ordinateurs portables intègrent une solution de chiffrement du disque dur : le cas échéant, il convient d'utiliser cette fonctionnalité.
- **Concernant les *smartphones*,** en plus du code PIN de la carte SIM, **activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller** (mot de passe, schéma, etc.).

### CE QU'IL NE FAUT PAS FAIRE

- Utiliser comme outil de sauvegarde ou de synchronisation les services *cloud* installés par défaut sur un appareil sans analyse approfondie de leurs conditions d'utilisation et des engagements de sécurité pris par les fournisseurs de ces services. Ceux-ci ne permettent généralement pas de respecter les préconisations données dans *la fiche n°13 : Gérer la sous-traitance.*

### POUR ALLER PLUS LOIN

- **Positionner un filtre de confidentialité** sur les écrans des postes utilisés dans des lieux publics.
- **Limiter le stockage des données** sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger (voir le « Passeport de conseils aux voyageurs » publié par l'ANSSI https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf).
- **Prévoir des mécanismes de protection contre le vol** (par ex. câble de sécurité, marquage visible du matériel) **et de limitation de ses impacts** (par ex. verrouillage automatique, chiffrement).
- Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex : assistants personnels, *smartphones*, ordinateurs portables, etc.), chiffrer les données sur le terminal. Prévoir aussi un verrouillage de l'appareil au bout de quelques minutes d'inactivité et la purge des données collectées sitôt qu'elles ont été transférées au système d'information de l'organisme.

# 7 PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE

## Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **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.

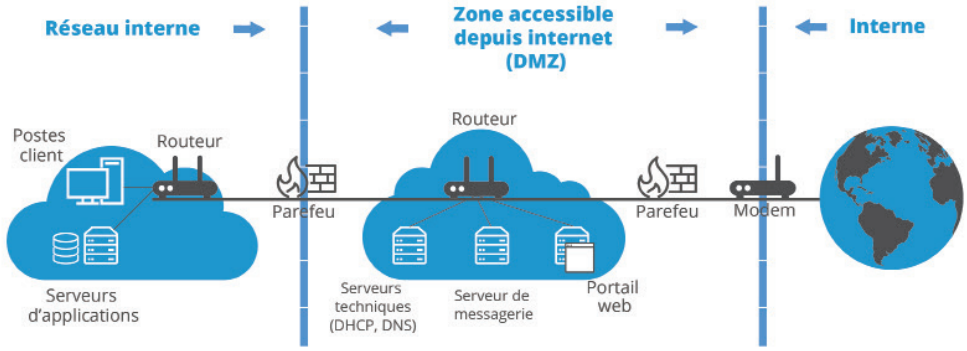
### CE QU'IL NE FAUT PAS FAIRE

- Utiliser le protocole telnet pour la connexion aux équipements actifs du réseau (pare-feu, routeurs, passerelles). Il convient d'utiliser plutôt SSH ou un accès physique direct à l'équipement.
- Mettre à disposition des utilisateurs un accès Internet non filtré.
- Mettre en place un réseau Wi-Fi utilisant un chiffrement WEP.

### POUR ALLER PLUS LOIN

- **L'ANSSI a publié[9] des recommandations** pour la sécurisation des sites web[10], TLS[11] et le Wi-Fi[12].
- **On peut mettre en place l'identification automatique de matériels en** utilisant les identifiants des cartes réseau (adresses MAC) afin d'interdire la connexion d'un dispositif non répertorié.
- **Des systèmes de détection d'intrusion** (IDS) peuvent analyser le trafic réseau pour détecter des attaques. Les utilisateurs doivent être avertis lorsque leurs contenus sont analysés.
- **Le cloisonnement réseau** réduit les impacts en cas de compromission. On peut distinguer un réseau interne sur lequel aucune connexion venant d'Internet n'est autorisée, et un réseau DMZ (DeMilitarized Zone) accessible depuis Internet, en les séparant par des passerelles (pare-feux).

**Exemple de mise en œuvre d'une DMZ**




9 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/.
10 https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/
11 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/
12 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/

# 8 SÉCURISER LES SERVEURS

## Renforcer les mesures de sécurité appliquées aux serveurs.

La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.**
  Utiliser des comptes de moindres privilèges pour les opérations courantes.
- **Adopter une politique spécifique de mots de passe** pour les administrateurs. Changer les mots de passe, au moins, lors de chaque départ d'un administrateur et en cas de suspicion de compromission.
- **Installer les mises à jour critiques** sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire
  En matière d'administration de bases de données ;
  - **utiliser des comptes nominatifs** pour l'accès aux bases de données et créer des comptes spécifiques à chaque application ;
  - mettre en œuvre des mesures contre les attaques par injection de code SQL, de scripts, etc.
- **Effectuer des sauvegardes et les vérifier régulièrement.**
- **Mettre en œuvre le protocole TLS** (en remplacement de SSL[13]), ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés[14].

### CE QU'IL NE FAUT PAS FAIRE

- Utiliser des services non sécurisés (authentification en clair, flux en clair, etc.).
- Utiliser pour d'autres fonctions les serveurs hébergeant les bases de données, notamment pour naviguer sur des sites web, accéder à la messagerie électronique, etc.
- Placer les bases de données sur un serveur directement accessible depuis Internet.
- Utiliser des comptes utilisateurs génériques (c'est-à-dire partagés entre plusieurs utilisateurs).

### POUR ALLER PLUS LOIN

- La recommandation de la CNIL[15] sur les mots de passe liste les bonnes pratiques à respecter.
- Tout système traitant de données sensibles[16] doit être mis en œuvre dans un **environnement dédié** (isolé).
- **Les opérations d'administration** des serveurs devraient se faire via **un réseau dédié et isolé**, accessible après une authentification forte et avec une traçabilité renforcée.
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels scanners de vulnérabilités tels que nmap[17] , nessus[18] , nikto[19], etc.) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés.
- Restreindre ou interdire l'accès physique et logique aux ports de diagnostic et de configuration à distance.
- **L'ANSSI a publié sur son site[20] diverses recommandations** parmis lesquelles la sécurisation de l'administration des systèmes d'information[21] et les bonnes pratiques en matière de sécurisation de l'annuaire central Active Directory[22].

13 Le protocole TLS est parfois appelé SSL ou SSL/TLS, « SSL » étant le nom donné à ce protocole pour ses premières versions considérées aujourd'hui comme vulnérables et à éviter.
14 Pour TLS, il existe par exemple https://www.ssllabs.com/ssltest/ ou https://ssl-tools.net/
15 https://www.cnil.fr/fr/mots-de-passe-des-recommandations-de-securite-minimales-pour-les-entreprises-et-les-particuliers
16 Les données sensibles sont décrites à l'article 8 de la loi informatique et libertés, et à l'article 9 du RGPD.
17 https://nmap.org/
18 http://www.nessus.org
19 http://www.cirt.net/nikto2
20 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/.
21 https://www.ssi.gouv.fr/entreprise/guide/securiser-ladministration-des-systemes-dinformation/
22 https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

9

# SÉCURISER LES SITES WEB

## S'assurer que les bonnes pratiques minimales sont appliquées aux sites web.

Tout site web doit garantir son identité et la confidentialité des informations transmises.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Mettre en œuvre le protocole TLS** (en remplacement de SSL[23]) 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.

### CE QU'IL NE FAUT PAS FAIRE

- Faire transiter des données à caractère personnel dans une URL telles que identifiants ou mots de passe.
- Utiliser des services non sécurisés (authentification en clair, flux en clair, etc.).
- Utiliser les serveurs comme des postes de travail, notamment pour naviguer sur des sites web, accéder à la messagerie électronique, etc.
- Placer les bases de données sur un serveur directement accessible depuis Internet.
- Utiliser des comptes utilisateurs génériques (c'est-à-dire partagés entre plusieurs utilisateurs).

### POUR ALLER PLUS LOIN

- Concernant la mise en œuvre de *cookies*, il est conseillé de consulter le dossier « *Site web, cookies et autres traceurs* » sur le site de la CNIL https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs.
- S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des **outils de détection des vulnérabilités** (logiciels scanners de vulnérabilité tels que nmap, nessus, nikto, etc.) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés. Ces tests doivent être menés de façon régulière et avant toute mise en production d'une nouvelle version logicielle.
- **L'ANSSI a publié sur son site[24] des recommandations spécifiques** pour mettre en œuvre TLS[25] ou pour sécuriser un site web[26].

23 Le protocole TLS est parfois appelé SSL ou SSL/TLS, « SSL » étant le nom donné à ce protocole pour ses premières versions considérées aujourd'hui comme vulnérables et à éviter.
24 https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
25 https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/
26 https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/

10

# SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ

## Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition non désirée de données.

Des copies de sauvegarde doivent être réalisées et testées régulièrement. Un plan de continuité ou de reprise d'activité anticipant les éventuels incidents (ex : panne matérielle) doit être préparé.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **S'agissant de la sauvegarde des données**
  - **Effectuer des sauvegardes fréquentes des données,** que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales[27] quotidiennes et des sauvegardes complètes à intervalles réguliers.
  - **Stocker les sauvegardes sur un site extérieur,** si possible dans des coffres ignifugés et étanches.
  - **Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation** (par exemple en chiffrant les sauvegardes, en prévoyant un stockage dans un lieu sécurité, en encadrant contractuellement une prestation d'externalisation des sauvegardes).
  - Lorsque les sauvegardes sont transmises par le réseau, il convient de chiffrer le canal de transmission si celui-ci n'est pas interne à l'organisme.
- **S'agissant de la reprise et de la continuité d'activité**
  - **Rédiger un plan de reprise et de continuité d'activité informatique** même sommaire, incluant la liste des intervenants.
  - **S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident.**
  - **Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.**
  - À propos des matériels :
    - utiliser un onduleur pour protéger le matériel servant aux traitements essentiels ;
    - prévoir une redondance matérielle des matériels de stockage, par exemple au moyen d'une technologie RAID[28].

### CE QU'IL NE FAUT PAS FAIRE

- Conserver les sauvegardes au même endroit que les machines hébergeant les données. Un sinistre majeur intervenant à cet endroit aurait comme conséquence une perte définitive des données.

### POUR ALLER PLUS LOIN

- Concernant l'établissement d'un plan de continuité d'activité ou de reprise d'activité, le SGDSN a publié un guide disponible à l'adresse : https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf.
- Si les exigences sur la disponibilité des données et des systèmes sont élevées, il est conseillé de mettre en place une réplication des données vers un site secondaire.

27 Une sauvegarde incrémentale consiste à n'enregistrer que les modifications faites par rapport à une précédente sauvegarde.
28 RAID (Redondant Array of Independant Disk) désigne des techniques de répartition de données sur plusieurs supports de stockage (par exemple des disques durs) afin de prévenir la perte de données consécutives à la panne d'un des supports.

11

# ARCHIVER DE MANIÈRE SÉCURISÉE

**Archiver les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux.**

Les archives doivent être sécurisées notamment si les données archivées sont des données sensibles ou des données qui pourraient avoir des impacts graves sur les personnes concernées.

## LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Définir un processus de gestion des archives :** quelles données doivent être archivées, comment et où sont-elles stockées, comment sont gérées les données descriptives ?
- **Mettre en œuvre des modalités d'accès spécifiques aux données archivées** du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle.
- S'agissant de la destruction des archives, **choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruite**.

## CE QU'IL NE FAUT PAS FAIRE

- Utiliser des supports ne présentant pas une garantie de longévité suffisante. À titre d'exemple, la longévité des CD et DVD inscriptibles dépasse rarement 4/5 années.
- Conserver les données en base active en les notant simplement comme étant archivées. Les données archivées ne doivent être accessibles qu'à un service spécifique chargé d'y accéder.

## POUR ALLER PLUS LOIN

La CNIL a publié une recommandation[29] concernant les modalités d'archivage électronique.

- Les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne soient pas détruites, sont régies par le livre II du Code du patrimoine. De plus amples informations sur les problématiques d'archivage sont disponibles sur le site des Archives de France. Voir, notamment l'article sur la pérennisation de l'information numérique[30] .
- En concertation avec la Direction générale des patrimoines du ministère de la Culture, la CNIL a publié l'autorisation unique n°29[31] qui encadre les traitements des services d'archives relatifs à des informations publiques contenant des données à caractère personnel.
- Le délégué et le comité interministériel aux archives de France animent et coordonnent l'action des administrations de l'État en matière d'archives. Dans ce cadre ils ont publié différents documents et référentiels, dont notamment le référentiel général de gestion des archives disponible à l'adresse : http://www.gouvernement.fr/delegue-et-comite-interministeriel-aux-archives-de-france.

29 https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651957
30 https://francearchives.fr/fr/article/26287479
31 https://www.cnil.fr/fr/declaration/au-029-archives-publiques

12

# ENCADRER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES

## Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.

Les opérations de maintenance doivent être encadrées pour maitriser l'accès aux données par les prestataires. Les données doivent être préalablement effacées des matériels destinés à être mis au rebut.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Enregistrer les interventions** de maintenance **dans une main courante**.
- Insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires.
- **Encadrer par un responsable de l'organisme les interventions par des tiers.**
- Rédiger et mettre en œuvre **une procédure de suppression sécurisée des données.**
- **Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparationchez un tiers** ou en fin du contrat de location.

### CE QU'IL NE FAUT PAS FAIRE

- Installer des applications pour la télémaintenance ayant des vulnérabilités connues, par exemple qui ne chiffrent pas les communications.
- Réutiliser, revendre ou jeter des supports ayant contenu des données à caractère personnel sans que les données n'aient était supprimées de façon sécurisée.

### POUR ALLER PLUS LOIN

- Utiliser des logiciels dédiés à la suppression de données sans destruction physique qui ont été audités ou certifiés. L'ANSSI accorde des certifications de premier niveau[32] à des logiciels de ce type.

**Exemple de clause pouvant être utilisés en cas de maintenance par un tiers :**

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à X.

En cas de télémaintenance permettant l'accès à distance aux fichiers de X, Y prendra toutes dispositions afin de permettre à X d'identifier la provenance de chaque intervention extérieure. À cette fin, Y s'engage à obtenir l'accord préalable de X avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de X et Y, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que les noms de leurs auteurs.

NB : Cette clause de maintenance doit nécessairement être couplée à celle traitant de la confidentialité pour la sous-traitance.



32 https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/

13

# GÉRER LA SOUS-TRAITANCE

## Encadrer la sécurité des données avec les sous-traitants.

Les données communiquées à des sous-traitants ou gérées par ces derniers doivent bénéficier de garanties suffisantes.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Faire appel uniquement à des sous-traitants présentant des garanties suffisantes** (notamment en termes de connaissances spécialisées, de fiabilité et de ressources). Exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information.
- Prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'**assurer l'effectivité des garanties offertes par le sous-traitant** en matière de protection des données. Ces garanties incluent notamment :
  - le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat ;
  - le chiffrement des transmissions de données (ex : connexion de type HTTPS, VPN, etc.) ;
  - des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.
- **Prévoir un contrat avec les sous-traitants**[33], qui définit notamment l'objet, la durée, la finalité du traitement et les obligations des parties. S'assurer qu'il contient en particulier des dispositions fixant :
  - leur obligation en matière de **confidentialité des données personnelles** confiées ;
  - des **contraintes minimales en matière d'authentification** des utilisateurs ;
  - **les conditions de restitution et/ou de destruction des données** en fin du contrat ;
  - **les règles de gestion et de notification des incidents**. Celles-ci devraient comprendre une information du responsable de traitement en cas de découverte de faille de sécurité ou d'incident de sécurité[34] et cela dans les plus brefs délais lorsqu'il s'agit d'une violation de données à caractère personnel.

### CE QU'IL NE FAUT PAS FAIRE

- Entamer la prestation de sous-traitance sans avoir signé un contrat avec le prestataire reprenant les exigences posées par l'article 28 du Règlement général sur la protection des données.
- Avoir recours à des services de *cloud* sans garantie quant à la localisation géographique effective des données et sans s'assurer des conditions légales et des éventuelles formalités auprès de la CNIL pour les transferts de données en dehors de l'Union européenne.

### POUR ALLER PLUS LOIN

- Consulter l'article 28 du règlement général sur la protection des données.
- Concernant le *cloud computing*, la CNIL a publié des recommandations ainsi que des propositions de clauses pour les contrats[35].
- Concernant les données de santé, un hébergeur doit disposer d'un agrément délivré par le ministère de la Santé[36]. Le référentiel de constitution d'un dossier est disponible sur le site du ministère de la santé[37]. À noter qu'une procédure de certification remplacera progressivement l'agrément des hébergeurs (voir l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel[38]).

33 La Cnil a publié un guide sous-traitant : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
34 Un incident de sécurité est caractérisé de « violation de données à caractère personnel » lorsqu'il touche à des données à caractère personnel.
35 https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services
36 Liste accessible sur http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees)
37 http://esante.gouv.fr/
38 https://www.legifrance.gouv.fr/eli/ordonnance/2017/1/12/2017-27/jo/texte

14

# SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES

## Renforcer la sécurité de toute transmission de données à caractère personnel.

**La messagerie électronique ne constitue pas un moyen de communication sûr** pour transmettre des données personnelles, sans mesure complémentaire. Une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des données personnelles et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, toute entité ayant accès aux serveurs de messagerie concernés (notamment ceux des émetteurs et destinataires) peut avoir accès à leur contenu.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers** (DVD, clé USB, disque dur portable).
- **Lors d'un envoi via un réseau :**
  - **chiffrer les pièces** sensibles à transmettre, si cette transmission utilise la messagerie électronique. À ce sujet, il convient de se référer aux préconisations de *la fiche n°17 – Utiliser des fonctions cryptographiques* ;
  - utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour lestransferts de fichiers, par exemple **SFTP** ou **HTTPS**, en utilisant **les versions les plus récentes des protocoles ;**
  - **assurer la confidentialité des secrets** (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).
- Si vous êtes amené à utiliser le **fax**, mettre en place les mesures suivantes :
  - installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité ;
  - faire afficher l'identité du fax destinataire lors de l'émission des messages ;
  - doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
  - préenregistrer dans le carnet d'adresse des fax (si la fonction existe) les destinataires potentiels.

### CE QU'IL NE FAUT PAS FAIRE

- Transmettre des fichiers contenant des données personnelles en clair via des messageries grand public.

### POUR ALLER PLUS LOIN

- L'utilisation d'algorithmes à clés publiques, lorsque les différents acteurs ont mis en place une **infrastructure de gestion de clés publiques,** apparaît particulièrement adaptée pour garantir la confidentialité et l'intégrité des communications, ainsi que l'authentification de l'émetteur.
- L'émetteur peut **signer électroniquement les données** avant leur envoi afin de garantir qu'il est à l'origine de la transmission *(voir fiche n°17)*.

15

# PROTÉGER LES LOCAUX

## Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.

L'accès aux locaux doit être contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- Installer des **alarmes anti-intrusion** et les vérifier périodiquement.
- **Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies,** et les inspecter annuellement.
- Protéger les clés permettant l'accès aux locaux et les codes d'alarme.
- **Distinguer les zones des bâtiments selon les risques** (par exemple prévoir un contrôle d'accès dédié pour la salle informatique).
- Tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone.
- **Établir les règles et moyens de contrôle d'accès** des visiteurs, au minimum en faisant **accompagner les visiteurs, en dehors des zones d'accueil du public**[35] par une personne appartenant à l'organisme.
- Protéger physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).

### CE QU'IL NE FAUT PAS FAIRE

- Sous-dimensionner ou négliger l'entretien de l'environnement des salles informatiques (climatisation, onduleur, etc.). Une panne sur ces installations a souvent comme conséquence l'arrêt des machines ou l'ouverture des accès aux salles (circulation d'air) neutralisant de facto des éléments concourant à la sécurité physique des locaux.

### POUR ALLER PLUS LOIN

- Conserver une trace des accès aux salles ou bureaux susceptibles d'héberger du matériel contenant des données personnelles pouvant avoir un impact négatif grave sur les personnes concernées. **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des représentants du personnel.
- Assurer que seul le personnel dûment habilité soit admis dans les zones à accès restreint.

Par exemple :

- à l'intérieur des zones à accès réglementé, exiger l**e port d'un moyen d'identification visible** (badge) pour toutes les personnes ;
- les visiteurs (personnel en charge de l'assistance technique, etc.) doivent avoir un accès limité. La date et l'heure de leur arrivée et départ doivent être consignées ;
- réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire.



39 Depuis leur entrée, pendant leur visite et jusqu'à leur sortie des locaux.

16

# ENCADRER LES DÉVELOPPEMENTS INFORMATIQUES

## Intégrer sécurité et protection de la vie privée au plus tôt dans les projets.

La protection des données à caractère personnel doit être intégrée au développement informatique dès les phases de conception afin d'offrir aux personnes concernées une meilleure maîtrise de leurs données et de limiter les erreurs, pertes, modifications non autorisée, ou mauvais usages de celles-ci dans les applications.

### LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Intégrer la protection de la vie privée, y compris ses exigences de sécurité des données, dès la conception** de l'application ou du service. Ces exigences peuvent se traduire par des choix d'architecture (décentralisée vs. centralisée), de fonctionnalités (anonymisation à bref délai, minimisation des données), de technologies (chiffrement des communications), etc.
- **Pour tout développement à destination du grand public, mener une réflexion sur les paramètres relatifs à la vie privée,** et notamment sur le paramétrage par défaut.
- **Éviter le recours à des zones de texte libre ou de commentaires.**
- Effectuer les développements informatiques et les tests dans un environnement informatique distinct de celui de la production (par exemple, sur des ordinateurs ou des machines virtuelles différents) et sur des données fictives ou anonymisées.

### CE QU'IL NE FAUT PAS FAIRE

- Utiliser des données à caractère personnel réelles pour les phases de développement et de test. Des jeux fictifs doivent être utilisés autant que possible.
- Développer une application puis réfléchir dans un second temps aux mesures de sécurité à mettre en place.

### POUR ALLER PLUS LOIN

- Le développement doit imposer des **formats de saisie et d'enregistrement des données qui minimisent les données collectées.** Par exemple, s'il s'agit de collecter uniquement l'année de naissance d'une personne, le champ du formulaire correspondant ne doit pas permettre la saisie du mois et du jour de naissance. Cela peut se traduire notamment par la mise en œuvre d'un menu déroulant limitant les choix pour un champ de formulaire.
- Les formats de données doivent être compatibles avec la mise en œuvre de la durée de conservation choisie. Par exemple, si un document numérique doit être conservé 20 ans, il pourrait être pertinent de privilégier des formats ouverts plus susceptibles d'être maintenus à long terme.
- La création et la gestion de profils utilisateurs donnant des droits d'accès aux données variant en fonction des catégories d'utilisateurs doit être intégrée dès les phases de développement.
- Un article dédié aux zones de texte libre ou de commentaires est accessible sur notre site CNIL[40].
- Selon la nature de l'application, il peut être nécessaire d'assurer son intégrité par le recours à des signatures du code exécutable garantissant qu'il n'a subi aucune altération.

17

# CHIFFRER, GARANTIR L'INTÉGRITÉ OU SIGNER

## Assurer l'intégrité, la confidentialité et l'authenticité d'une information.

Les **fonctions de hachage** permettent d'assurer **l'intégrité des données. Les signatures numériques,** en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité. Enfin, **le chiffrement,** parfois improprement appelé cryptage, permet de garantir **la confidentialité** d'un message.

## LES PRÉCAUTIONS ÉLÉMENTAIRES

- **Utiliser un algorithme reconnu et sûr,** par exemple, les algorithmes suivants :
  - SHA-256, SHA-512 ou SHA-3[41] comme fonction de hachage ;
  - HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2 pour stocker les mots de passe;
  - AES ou AES-CBC pour le chiffrement symétrique ;
  - RSA-OAEP comme défini dans PKCS#1 v2.1 pour le chiffrement asymétrique ;
  - enfin, pour les signatures, RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1.
- **Utiliser les tailles de clés suffisantes**[42], pour AES il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536.
- **Protéger les clés secrètes,** au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr.
- **Rédiger une procédure indiquant la manière dont les clés et certificats vont être gérés** en prenant en compte les cas d'oubli de mot de passe de déverrouillage.

## CE QU'IL NE FAUT PAS FAIRE

- Utiliser des algorithmes obsolètes, comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA1.
- Confondre fonction de hachage et chiffrement et considérer qu'une fonction de hachage seule est suffisante pour assurer la confidentialité d'une donnée. Bien que les fonctions de hachages soient des fonctions « à sens unique », c'est à dire des fonctions difficiles à inverser, une donnée peut être retrouvée à partir de son empreinte. Ces fonctions étant rapides à utiliser, il est souvent possible de tester automatiquement toutes les possibilités et ainsi de reconnaître l'empreinte.

## POUR ALLER PLUS LOIN

- « Comprendre les grands principes de la cryptologie et du chiffrement » accessible à l'adresse https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement.
- Lors de la réception d'un certificat électronique, **vérifier que le certificat** contient une indication d'usage conforme à ce qui est attendu, qu'il **est valide et non révoqué, et qu'il possède une chaîne de certification correcte** à tous les niveaux.
- **Utiliser des logiciels ou des bibliothèques cryptographiques ayant fait l'objet de vérifications par des tierces parties à l'expertise avérée.**
- Différentes solutions de chiffrement peuvent être utilisées, tels que :
  - les solutions certifiées ou qualifiées par l'ANSSI[43];
  - le logiciel VeraCrypt, permettant la mise en œuvre de conteneurs[44] chiffrés ;
  - le logiciel GNU Privacy Guard, permettant la mise en œuvre de la cryptographie asymétrique (signature et chiffrement)[45].

41 SHA-256 comme définies dans le FIPS 180-2.
42 Un état de l'art en la matière est disponible dans les annexes du référentiel général de sécurité publié par l'ANSSI sur son site.
43 https://www.ssi.gouv.fr/entreprise/ aux rubriques certification et qualification
44 Par conteneur, il faut comprendre un fichier susceptible de contenir plusieurs fichiers.
45 https://www.gnupg.org/index.fr.html

# ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

## Avez-vous pensé à ?

| FICHES | | MESURE | |
|---|---|---|---|
| 1 | Sensibiliser les utilisateurs | Informez et sensibilisez les personnes manipulant les données | ☐ |
| | | Rédigez une charte informatique et lui donner une force contraignante | ☐ |
| 2 | Authentifier les utilisateurs | Définissez un identifiant (login) unique à chaque utilisateur | ☐ |
| | | Adoptez une politique de mot de passe utilisateur conforme à nos recommandations | ☐ |
| | | Obligez l'utilisateur à changer son mot de passe après réinitialisation | ☐ |
| | | Limitez le nombre de tentatives d'accès à un compte | ☐ |
| 3 | Gérer les habilitations | Définissez des profils d'habilitation | ☐ |
| | | Supprimez les permissions d'accès obsolètes | ☐ |
| | | Réaliser une revue annuelle des habilitations | ☐ |
| 4 | Tracer les accès et gérer les incidents | Prévoyez un système de journalisation | ☐ |
| | | Informez les utilisateurs de la mise en place du système de journalisation | ☐ |
| | | Protégez les équipements de journalisation et les informations journalisées | ☐ |
| | | Prévoyez les procédures pour les notifications de violation de données à caractère personnel | ☐ |
| 5 | Sécuriser les postes de travail | Prévoyez une procédure de verrouillage automatique de session | ☐ |
| | | Utilisez des antivirus régulièrement mis à jour | ☐ |
| | | Installez un « pare-feu » (*firewall*) logiciel | ☐ |
| | | Recueillez l'accord de l'utilisateur avant toute intervention sur son poste | ☐ |
| 6 | Sécuriser l'informatique mobile | Prévoyez des moyens de chiffrement des équipements mobiles | ☐ |
| | | Faites des sauvegardes ou synchronisations régulières des données | ☐ |
| | | Exigez un secret pour le déverrouillage des smartphones | ☐ |
| 7 | Protéger le réseau informatique interne | Limitez les flux réseau au strict nécessaire | ☐ |
| | | Sécurisez les accès distants des appareils informatiques nomades par VPN | ☐ |
| | | Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi | ☐ |
| 8 | Sécuriser les serveurs | Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées | ☐ |
| | | Installez sans délai les mises à jour critiques | ☐ |
| | | Assurez une disponibilité des données | ☐ |
| 9 | Sécuriser les sites web | Utilisez le protocole TLS et vérifiez sa mise en œuvre | ☐ |
| | | Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url | ☐ |
| | | Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu | ☐ |
| | | Mettez un bandeau de consentement pour les *cookies* non nécessaires au service | ☐ |
| 10 | Sauvegarder et prévoir la continuité d'activité | Effectuez des sauvegardes régulières | ☐ |
| | | Stockez les supports de sauvegarde dans un endroit sûr | ☐ |
| | | Prévoyez des moyens de sécurité pour le convoyage des sauvegardes | ☐ |
| | | Prévoyez et testez régulièrement la continuité d'activité | ☐ |
| 11 | Archiver de manière sécurisée | Mettez en œuvre des modalités d'accès spécifiques aux données archivées | ☐ |
| | | Détruisez les archives obsolètes de manière sécurisée | ☐ |
| 12 | Encadrer la maintenance et la destruction des données | Enregistrez les interventions de maintenance dans une main courante | ☐ |
| | | Encadrez par un responsable de l'organisme les interventions par des tiers | ☐ |
| | | Effacez les données de tout matériel avant sa mise au rebut | ☐ |
| 13 | Gérer la sous-traitance | Prévoyez une clause spécifique dans les contrats des sous-traitants | ☐ |
| | | Prévoyez les conditions de restitution et de destruction des données | ☐ |
| | | Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.) | ☐ |
| 14 | Sécuriser les échanges avec d'autres organismes | Chiffrez les données avant leur envoi | ☐ |
| | | Assurez-vous qu'il s'agit du bon destinataire | ☐ |
| | | Transmettez le secret lors d'un envoi distinct et via un canal différent | ☐ |
| 15 | Protéger les locaux | Restreignez les accès aux locaux au moyen de portes verrouillées | ☐ |
| | | Installez des alarmes anti-intrusion et vérifiez-les périodiquement | ☐ |
| 16 | Encadrer les développements informatiques | Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux | ☐ |
| | | Évitez les zones de commentaires ou encadrez-les strictement | ☐ |
| | | Testez sur des données fictives ou anonymisées | ☐ |
| 17 | Utiliser des fonctions cryptographiques | Utilisez des algorithmes, des logiciels et des bibliothèques reconnues | ☐ |
| | | Conservez les secrets et les clés cryptographiques de manière sécurisée | ☐ |